MICROgarde I & II

access control system

and MICROgarde software

User Guide

UM0060 GB Issue 3 10/02/2012

www.tdsi.co.uk

TDSi
Unit 10 Concept Park
Innovation Close
Poole
Dorset
BH12 4QT, UK

Tel: +44 (0) 1202 723535
Fax: +44 (0) 1202 724975

Sales Enquiries: sales@tdsi.co.uk
General Enquiries: info@tdsi.co.uk
Marketing Support: marketing@tdsi.co.uk
Technical Support: support@tdsi.co.uk

Foreword

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Trademarks

Copyright © 2012 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied nor shall any part of it be reproduced without the prior written consent of TDSi.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Cautions and Notes

The following symbols are used in this guide:

⚠ **CAUTION! This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.**

ℹ **NOTE.** This indicates important information to help you make the best use of this product.

Contents

Figures

Tables

1. Introduction

Thank you for purchasing your TDSi MICROgarde door access control system.

There are 2 main types of MICROgarde controller (often referred to as MG controllers) the MICROgarde I and MICROgarde II. MICROgarde I is a 1-door controller with connections for 1-2 readers. MICROgarde II is a 2-door controller with connections for up to 4 readers.

The controllers can operate independently or as part of a networked system all administered from a single computer (PC) using the supplied MICROgarde software. In addition, spare inputs and relays are available for monitoring and control of other equipment.

MICROgarde's key features are:

- One- or two-door access control unit
- Network to 200 other MICROgarde units
- Up to 800 TDSi or 400 third-party readers
- Built-in RS-232/RS-485 converter
- Reversible 2-wire RS-485 communication
- Variable lock times
- Diagnostic LEDs
- Additional I/O and TCP/IP modules available
- Automatic fire door release
  (not to be used as the primary method of releasing fire doors)
- Full compatibility with EXgarde PRO providing an easy upgrade path for enhanced functionality
- Intuitive software
- Automated database backup
- Custom reporting feature

This manual will guide you through the installation of MICROgarde I & II controllers (with or without integral power supply) and explain the operation of the TDSi MICROgarde administration and monitoring software. There is a Troubleshooting section starting on page 89.

1.1 System Components

This section describes the key components of a MICROgarde system.

1.1.1 MICROgarde controller (I or II)

- 1 or 2-door, 2 – 4 reader controllers (2 readers only with non-TDSi readers)
- 2 changeover lock relays *
- 2 Door sense and 2 Egress inputs *
- On-board memory and intelligence
- Built-in tamper detection
- RS232, RS485 or TCP/IP communications
- Built-in RS232/RS485 converter
- Built-in RS485 line termination
- Auto reader-type detection
- Rotary switch for unit-number selection

* When used for controlling only one door, one relay and two inputs become spare for monitoring and control of other devices.

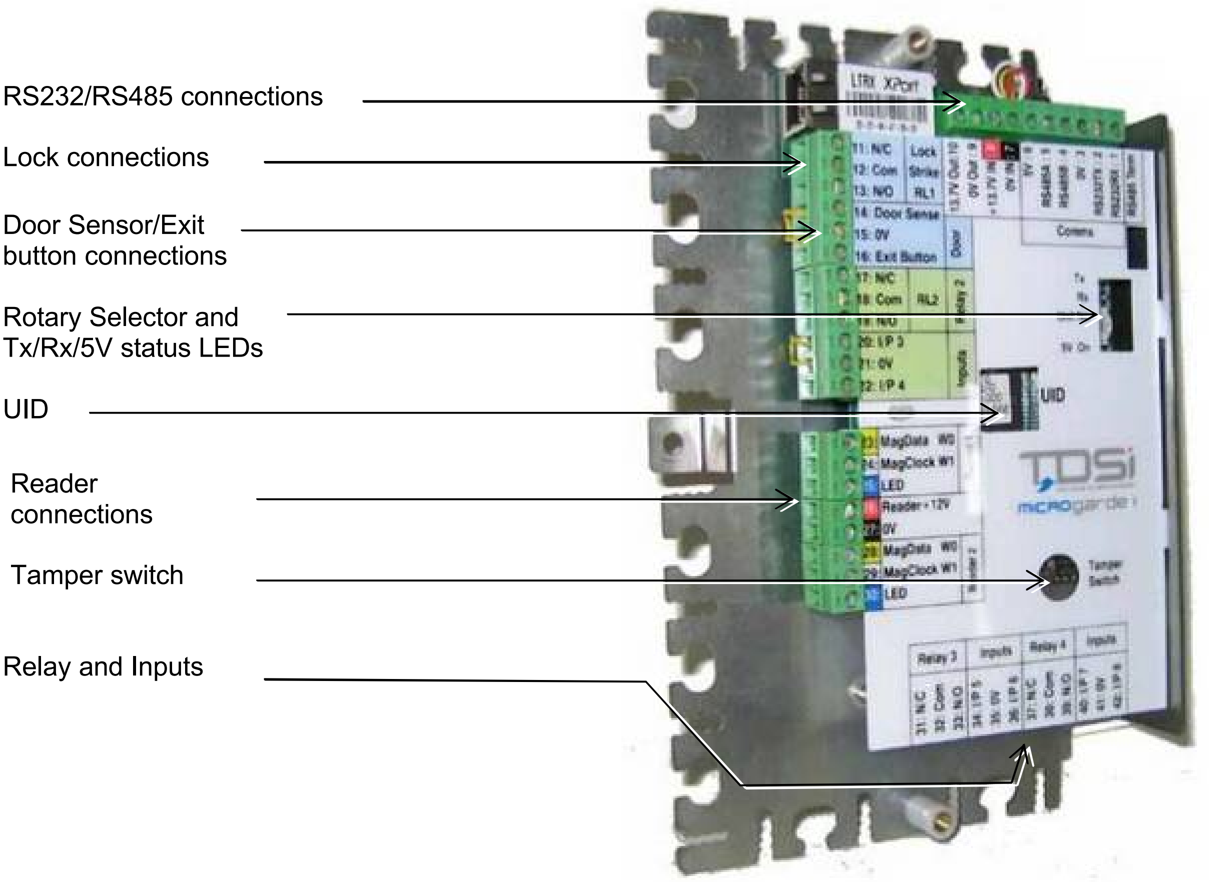


Figure 1 MICROgarde Controller

1.1.2 Readers

Choose from proximity (Mifare, Wiegand or clock and data), mag-stripe, digital infra-red or biometric technologies.

1.1.3 Cards

All cards are available as plain white standard sized cards suitable for use in Photo-ID badge printers. Proximity, infra-red, long range key-fobs are available as a convenient alternative to cards. TDSi can supply a full range of technologies to meet your business requirement from 125KHz proximity to 13.56MHz smart card with integrated contact chip.

- Standard and custom cards supplied
- Choice of card or key fob
- Multi technology available
- Custom printing if required
- Combine physical and logical access control

1.1.4 Options

I/O board option

Adds 4 inputs and 2 change-over relays to a MICROgarde controller

TCP/IP Port option

Adds a 10/100 Mb Ethernet port to a MICROgarde controller, MICROgarde then converts for 2-wire RS485 to other controllers

RS232/RS485 Converter

MICROgarde controller converts an RS232 from PC to 2-wire RS485 out to other controllers. RS232 supports max. 15m if greater distance is required than can use alternative converters.

USB/RS485 Converter

For direct RS485 control from the PC, a USB to RS485 converter may be used to connect to the controllers.

1.1.5 MICROgarde Explorer

MICROgarde Explorer is TDSi's Windows-based software application for use with up to 200 networked controllers. The software only supports MICROgarde controllers but you can upgrade to EXgarde Pro software. Contact TDSi for details.

1.2 Overview

1.2.1 Access control

Each person who is to be allowed access is given a card (or key fob) with a unique number. When the card is presented at a reader next to a door, the number is read and transmitted to the MICROgarde controller to which it is connected. If that number is in the memory of the controller, with permission to enter the door at that time, the controller operates a relay which in turn unlocks the door for a preset number of seconds. The controller also records the event, which is sent to the software event trail and logging.

MICROgarde software is used to set up a system of up to 200 MICROgarde controllers. Once the system is set up, the software can be closed down if required because each controller contains all of the valid card numbers together with all the rules that govern access.

The software will also retrieve and display events as they happen. If events have occurred while the software has been closed down, the software will retrieve them when re-started. If a controller records 1000 events (programmable) while it is off-line then the oldest event is discarded to make room for each new event.

1.2.2 Doors and readers

There are 2 main types of MICROgarde controller: MICROgarde I and MICROgarde II.

- MICROgarde I is a 1 door controller with 1-2 readers.
- MICROgarde II is a 2 door controller with up to 4 TDSi readers or two non-TDSi readers.

A door can have a reader on both sides of the door. Because a card holder is given permission (courtesy of his or her access level) on a reader-by-reader basis, a card may be allowed access through a door in one direction only if required. Where a reader is fitted on one side of the door only, opening the door from the other side may require the fitting of suitable door hardware or an exit button.

1.2.3 Inputs and relays

You can reduce the number of doors controlled by a MICROgarde and thus use the spare relays and inputs for monitoring other devices. An optional board can be added to each controller that adds 4 more spare inputs and 2 relay outputs.

If required a MICROgarde can be programmed to be pure I/O and not used for reader and door. A MICROgarde II with an I/O board fitted would provide 4 spare relays and 8 spare inputs in total.

An input can be connected to another device that contains (or behaves like) a switch. For example, a contact fitted to a window frame could be connected so that you could see in the MICROgarde software whether the window was open, and also see the times of opening and closing.

A relay can be connected to another device for the purpose of turning it on and off in the following ways:

- From an instruction by the Operator using the software
- Automatically when an input is switched on and off

- Automatically according to a pre-set time pattern

1.2.4 Options

The simplest possible system, in addition to the PC running the software, would comprise 1 controller, 1 reader, one 12V power supply (for both lock and controller) and one electric lock release. The following extras are available, some of which may be required depending on site layout and cable distances:

Lock Power supply

We recommend the use of separate power supplies for locks. In most cases however, using one supply for the controller and the lock(s) it controls will cause no problems provided the supply has sufficient current output, and the cable distances do not result in significant voltage drops. If in doubt, use one supply for the controller, and one supply for each lock.

Door sensor

Using a switch to detect when a door opens has two possible benefits:

- It minimizes the length of time the door is unlocked after access has been granted. The door locks immediately it re-closes - regardless of the "lock release time" setting.
- The event list shows when doors open and close. If an exit reader or exit button is fitted, the event list shows if the door is forced open (i.e. opens without either a card or an exit button being used).

Exit button

Depending on the type of lock release, fitting an exit button may be the most convenient way of letting someone out of a secured area if no exit reader is fitted. Pressing the button causes the lock to be released just as if a card had been used.

Exit reader

If you want to monitor the whereabouts of all card holders, fitting an exit reader is necessary. You can set reader properties so that you can see whether card holders are "On Site" or not.

Readers with keypads

There is always a risk that someone can gain access with a lost or stolen card, if the card is used before it is deleted from the system. However, if a reader has a keypad fitted, then it is possible to require a code to be entered as well as the card and this increases security because only the rightful card holder should know the code for that card.

Alternatively you can reduce security by using just a pin only code. It is possible to have weekly schedules of card and pin; card only and pin only.

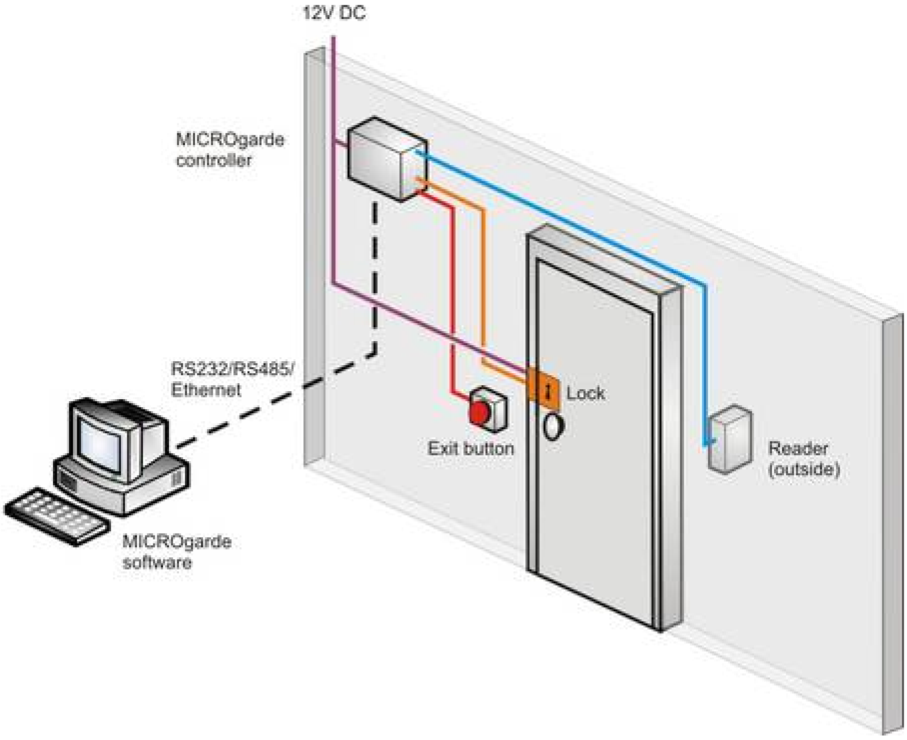


Figure 2 **Simple, single door, access system using MICROgarde I**
(no door sensor, single reader with Exit button, single 12 V supply for access unit and lock)

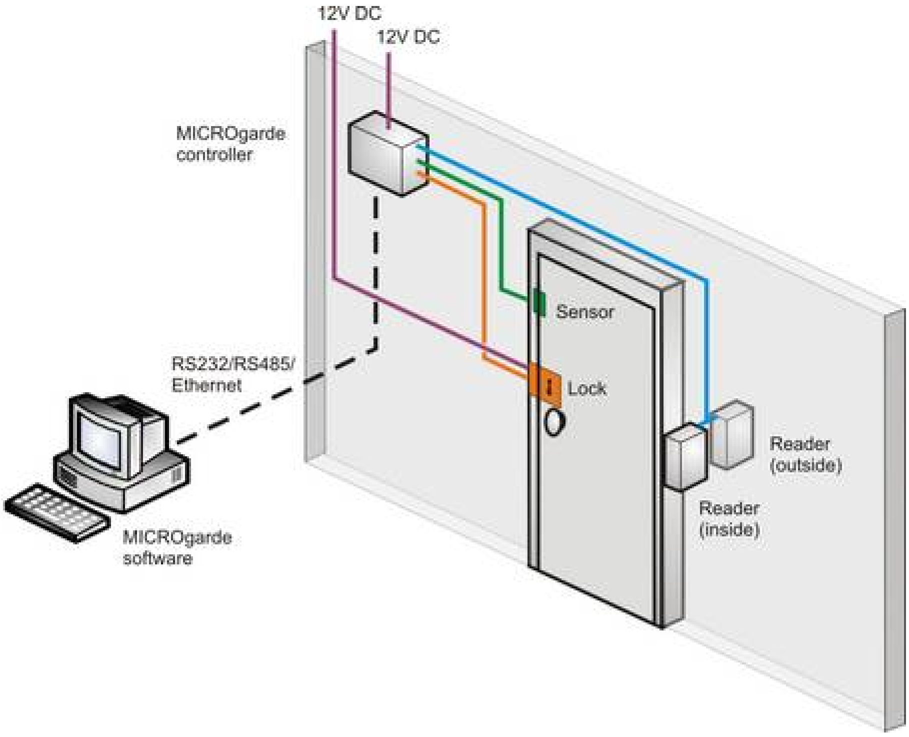


Figure 3 **Full, single door, access system using MICROgarde I**
(door sensor, inside and outside readers, Exit button, separate 12 V supplies for access unit and lock)

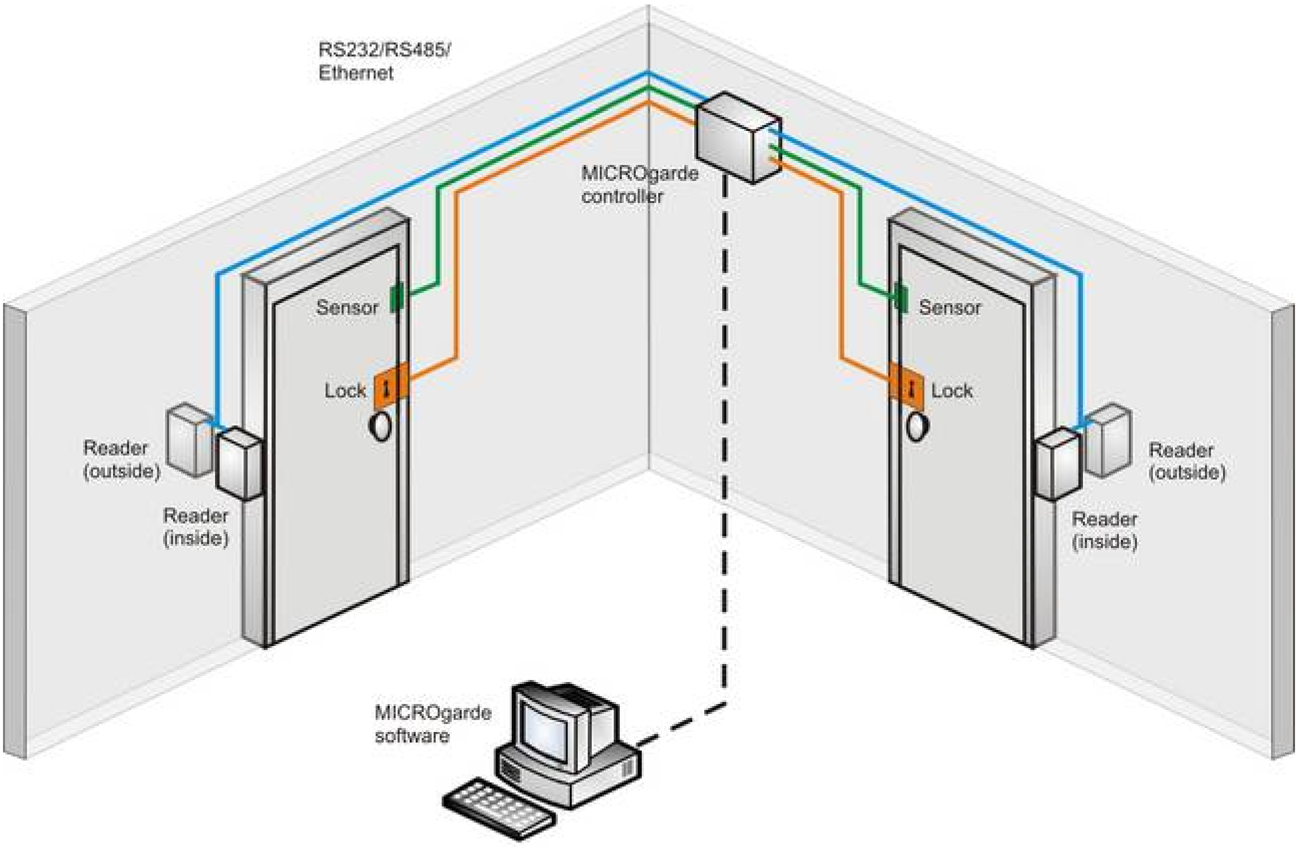


Figure 4 Two door access system using MICROgarde II
(12V DC power supplies for access unit and locks not shown)

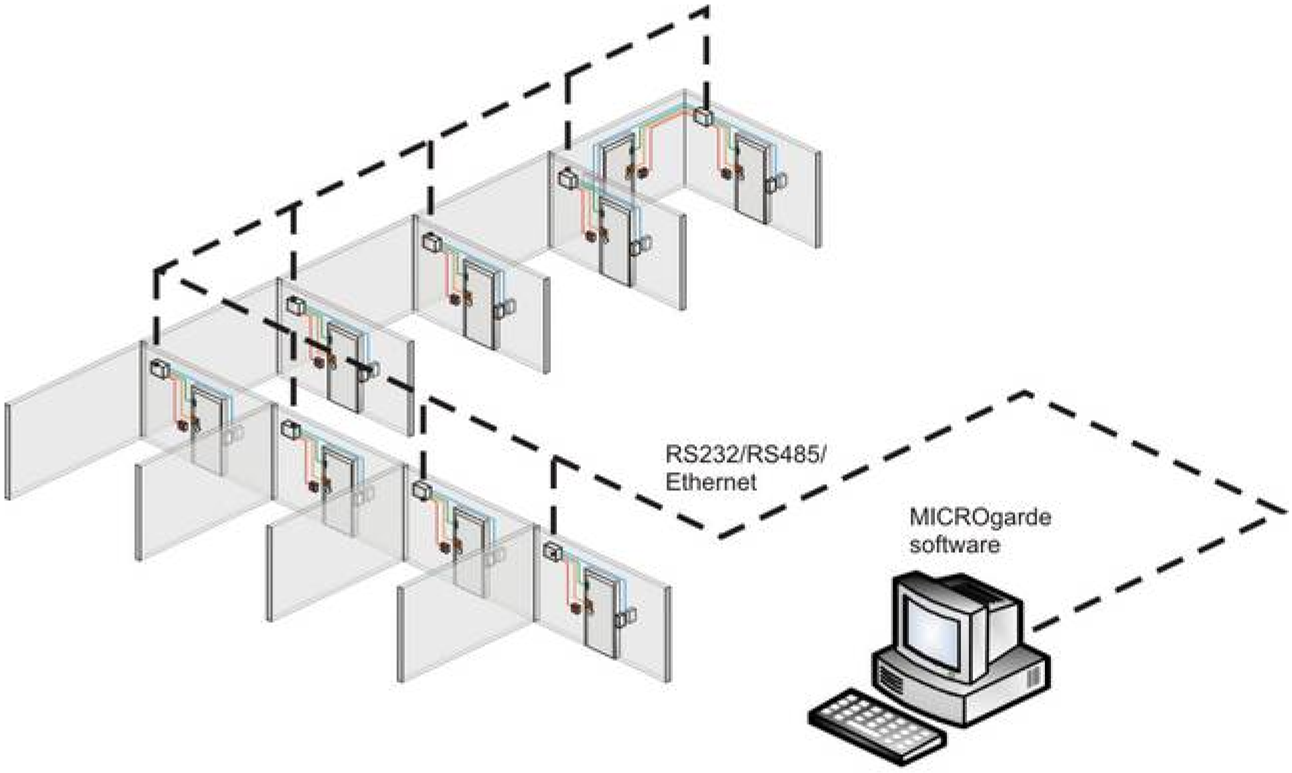


Figure 5 MICROgarde network

2. Installation

2.1 What's in the box

1 x MICROgarde controller (with or without PSU depending on order)

1x Polythene bag containing: 3 x screws, 3 x raw plugs, 1 x tamper spring, 2 x ceramic capacitors for mains filter and

2 x diode suppressors

1x Quick Install guide

WARNING! Lock strike suppression devices (2 DIODE SUPPRESSORS ARE SUPPLIED) MUST be fitted directly across all inductive loads such as lock strikes, secondary relays and automatic door openers. Failure to adhere to this notice will invalidate the warranty of this product and may result in irreparable damage to it and other connected equipment.

2.2 Physical Installation

The MICROgarde controller is designed to be mounted on flat (or nearly-flat) surfaces while allowing cables to pass underneath. Three screws are required to mount the chassis onto the wall.

The acceptable temperature range for the controller is -5°C to +50°C. The controller generates some heat and the ambient temperature where the controller is installed may rise without adequate ventilation.

2.3 Cabling Requirements

All communications and reader cables should be in screened cable and at least two metres long for full EMC protection and maximum reliability.

2.3.1 Choosing the correct cable

Note. TDSI recommends using screened cable throughout for ALL cables including door sensors, exit buttons, inputs and lock.

Connections to the power supply and any readers MUST use screened cables. With communications cables, you are strongly recommended to use a screened cable.

Table 1 lists the recommended cable types.

Table 1 Recommended cable types

Component	Part No.	Cable Type	Cores	Maximum Distance
Magnetic Stripe Reader	5002-0360	Belden 9730	6	60m
		Belden 9503	6	25m
		OS6C24/Alpha 5096/BICC H8124	6	20m
		Screened Alarm Cable	8	Up to 30m
EXprox / EXprox2	5002-0354 5002-0355	Belden 9730	6	150m
		Belden 9503	6	150m
		OS6C24/Alpha 5096/BICC H8124	6	150m
		Screened Alarm Cable	8	150m
Optica	5002-0390 5002-0391	Belden 9730	6	150m
		Belden 9503	6	150m
		OS6C24/Alpha 5096/BICC H8124	6	150m
		Screened Alarm Cable	8	150m
Digital IR	5002-1781 5002-1791	Belden 9730	6	150m
		Belden 9503	6	150m
		OS6C24/Alpha 5096/BICC H8124	6	150m
		Screened Alarm Cable	8	150m
MIFARE / EXsmart2	5002-0433 5002-0434 5002-0435 5002-0436 5002-0440	Belden 9730	6	150m
		Belden 9503	6	150m
		OS6C24/Alpha 5096/BICC H8124	6	150m
		Screened Alarm Cable	8	150m
DIGIgarde / DIGIgarde Smart / PALMgarde	5002-0450 5002-0451 5002-0460	Belden 9730	6	150m
		Belden 9503	6	150m
		OS6C24/Alpha 5096/BICC H8124	6	150m
		Screened Alarm Cable	8	150m
Indala Proximity Reader	5002-0133 5002-0137 5002-0217 5002-0218	Belden 9730	6	150 m
		Belden 9503	6	60 m
		OS6C24/Alpha 5096/BICC H8124	6	60 m
		Screened Alarm Cable	8	Up to 30m
Dataline Keypad	5002-0286 5002-0315 5002-0316	Belden 9729	4	140m
		FBOS2P24	4	100m
		OS2P22/Alpha 5902/Belden 9502	4	60m
		OS4C24/Alpha 5094/BICC H8123	4	40m
RS-232		7/0.2 mm 3– core screened cable	3	15m
RS-485 [1]		Belden 9729	4	1200m
		FBOS2P24	4	900m
		OS2P22/Alpha 5902/Belden 9502	4	530m
		OS4C24/Alpha 5094/BICC H8123	4	400m
		Screened Alarm Cable	8	300m
Inputs		7/0.2mm (screened)	2	300m
Relays		7/0.2mm or 16/0.2mm (screened)	2	Dependent on load and cable choice

[1] Up to 32 MICROgarde access control units can be connected to a single port.

2.3.2 Grounding

Always ensure the MICROgarde chassis is connected to a GOOD earth grounding.

In general, the communication and other peripheral cable screens should be earthed at the MICROgarde chassis ONLY. The one exception to this rule is if the item (e.g. reader, egress, lock etc.) is mounted on an earthed metal surface. In this instance, earth the cable to the metal surface and NOT at the MICROgarde unit. This prevents earth loops which can allow current to flow along the screen wire causing interference.

Keep all unshielded cable runs and earth/drain wire “pig tails” as short as possible. To minimize exposed earth braid, never remove more cable sheathing than necessary.

Figure 6 shows the correct way to feed cables around the slots in the chassis plate. It is important that the cable screens are tightly gripped – a thin, single cable can be folded back on itself and twisted to thicken it, or it can be wrapped round the metal between two slots.

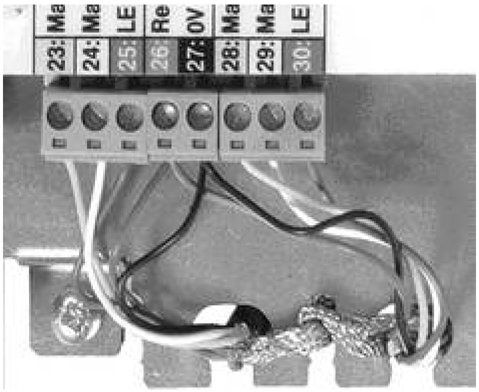


Figure 6 Securing cables through the chassis plate

2.4 Connections

CAUTION! Please read this section carefully as incorrect wiring could cause irreparable damage to the controller and invalidate the warranty. Check all wiring before connecting power to the unit.

2.4.1 Connecting Readers

The MICROgarde controller can be connected to any make or type of reader using the following communication protocols:

- Clock&Data (Magnetic)
- Wiegand:
    - Standard 26 bit
    - HID 37 bit
    - Generic Wiegand variable up to 28 Bits

Note. TDSi readers such as the eXprox, eXprox VR, and TDSi MIfare have colour-coded wires that match the MICROgarde connections overlay label.

To use 2 readers on each channel for In and Out readers on the same door, then you must be using one of the following readers: EXprox, EXprox VR, Optica, Optica VR, Digital IR, EXprox 2, EXprox 2K, EXsmart 2 or EXsmart 2K.

For readers 3 and 4 using EXprox and Digital IR, fit the extra brown wire to CLOCK, for other TDSi readers please refer to its manual.

CAUTION! Use shielded cable for all readers.

2.4.2 Egress or Exit button

Note. If you have connected readers on both sides of a single door this option may not be necessary.

Use switches with voltage-free contacts: a simple short triggers the egress function.

2.4.3 Door sensor

Use a door sensor if you want to know when the door is opened normally, forced open, or left open too long. MICROgarde can be programmed to associate either an open or closed circuit with the open/closed door position (see page 38).

Use sensors with voltage-free contacts as a simple short triggers the function.

2.4.4 Lock and Lock PSU connection

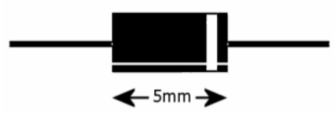
CAUTION! A suppressor MUST be fitted at each lock (see below). Two suitable suppressors (1N4003 diodes) are provided with each MICROgarde controller.

For maximum reliability, we recommend the use of separate power supplies for locks. In most cases however, using one supply for the controller and the lock(s) it controls will cause no problems provided the supply has sufficient current output, and the cable distances do not result in significant voltage drops. If in doubt, use one supply for the controller, and one supply for each lock.

For each lock, allow 50% more than its stated rating. For example, if the lock has a rating of 500mA, use a 750mA minimum supply. If the lock has a higher current rating than the lock relay (2A), use a secondary relay.

Always run the power to the lock in a separate cable.

Fitting a suppressor



Fit the supplied suppressor across the lock supply as close to the lock as possible (NOT at the MICROgarde unit) with the white band end connected to the positive side of the supply. The supplied suppppressors are suitable for DC locks ONLY.

– the suppressor must be connected across the two wires

Fail safe lock connection

Figure 7 shows the connections for a “fail-safe” lock, i.e. when the power is off, the door is unlocked. Connect the supply of the lock across the **N/O** (normally OPEN) and the **Com** (Common). When the relay is triggered to allow access, it supplies power to the lock.

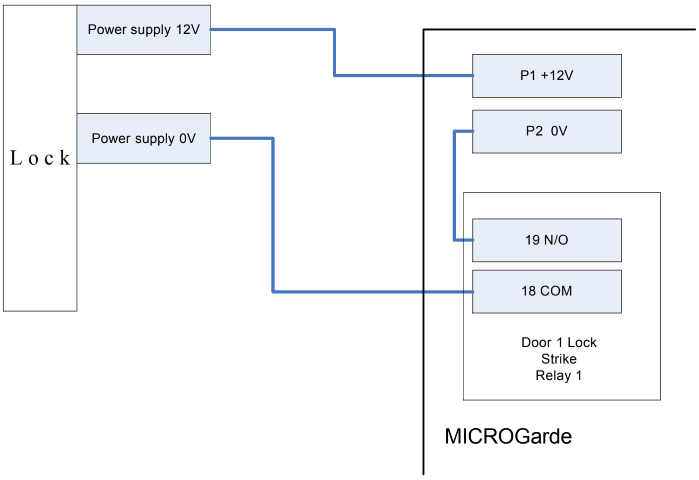


Figure 7 Connecting a fail-safe lock

2.4.5 Power Supply connection

MICROgarde units without integral PSU

If you have purchased a MICROgarde unit without an integral power supply, you need to connect the unit to a suitable PSU. This should be capable of supplying enough power for the controller and its readers. In most cases, a 1A power supply is adequate. However, if your installation consists of 4 Optica readers/keypads and a TCP/IP module, you should use a 1.5A supply.

1. Connect the PSU to the MICROgarde's **0V** and **12V** terminals using braid-screened cable. Position the PSU as close as possible to the unit.
2. To minimize electrical interference, ensure that the MICROgarde and PSU are grounded together: fasten the braid screen to both the main earth point in the PSU and to the chassis plate of the MICROgarde.
3. Fit two suppressors across the mains input to the power supply. Suitable suppressors are provided with each MICROgarde non PSU unit. These are 470 pF (pico-Farad) Class Y disc ceramic capacitors rated at 240V AC.

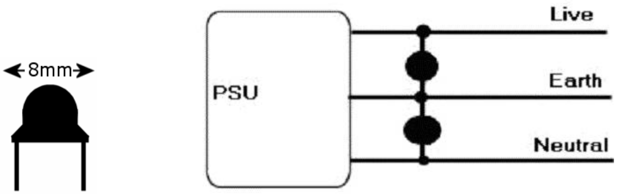


Figure 8 (a) Appearance and dimensions of PSU suppressor and (b) connection to PSU

MICROgarde units with integral PSU

A MICROgarde controller with integral PSU features a high-quality 2A power supply unit with separate 1A outputs for the door controller and the lock.

The lock power MUST be taken from the terminal block on the power supply shown below and not from the power terminals (7, 8, 9 and 10) on the MICROgarde controller. Failure to do so may result in unreliable operation of the door controller.

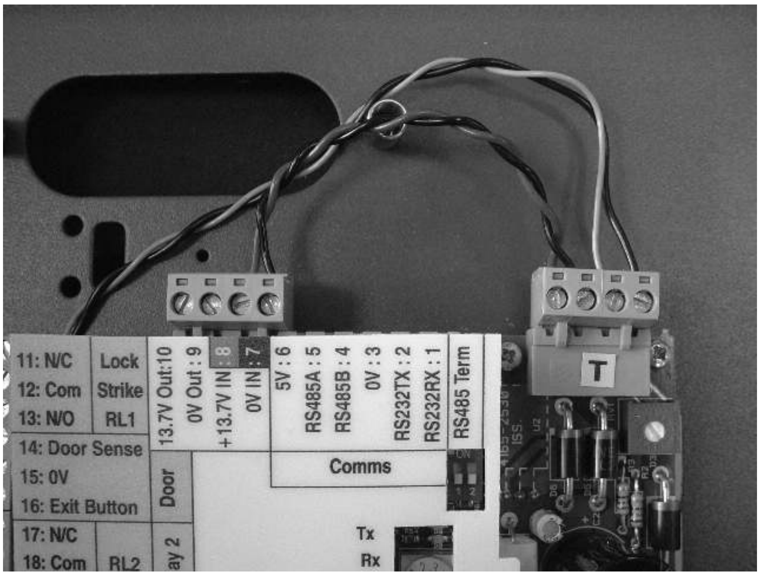


Figure 9 Lock power must be taken from the fused output terminals

2.4.6 Communications

Earthing

The communications cable should be earthed on the incoming side only: the cable bringing communications in from the administration computer or the preceding MICROgarde unit or other Access Control Unit (ACU). The communications cable leaving the ACU should ideally be taped off. (This prevents earth loops).

For RS485 termination, put the termination dip switches 1 and 2 ON. Do this only on the first MICROgarde controller in the RS485 bus.

RS232 communication

Note. This method is only suitable if the administration PC is within 15m of the MICROgarde unit and has a vacant COM port. If the administration PC is more than 15m from a MICROgarde unit and you want to use RS232, you will need to use an RS232/RS485 converter. The TDSI RS232 to 2-wire RS485 Converter can be used for this purpose – part no. 5012-0013 (UK plug) or 5012-0014 (Euro Plug).

Create an RS232 link as described in Table 2 and shown in Figure 10.

Table 2 Networking a PC to a MICROgarde using RS232

RS232 Pin	MICROgarde pin	Colour*
2	2 – RS232 Tx	Red
3	1 – RS232 Rx	Blue
5	3 - 0V	Green

*TDSi RS232 comms lead (5002-1813) only.
Other manufacturers may use different colour coding.

To create a network, you can connect further MICROgarde units from connections 4 & 5. These connections use RS485 but the MICROgarde has a built-in RS485/RS232 conversion capability. Up to a maximum of 31 MICROgarde controllers can be added in this way. Ensure you use a continual line or “daisy chain” with no spurring.

Note. 4-core RS485 cable is often cheaper and more easily obtained than 2-core. If you use 4-core cable, connect the cores together in pairs, using one core from each pair – do not leave cores un-connected.

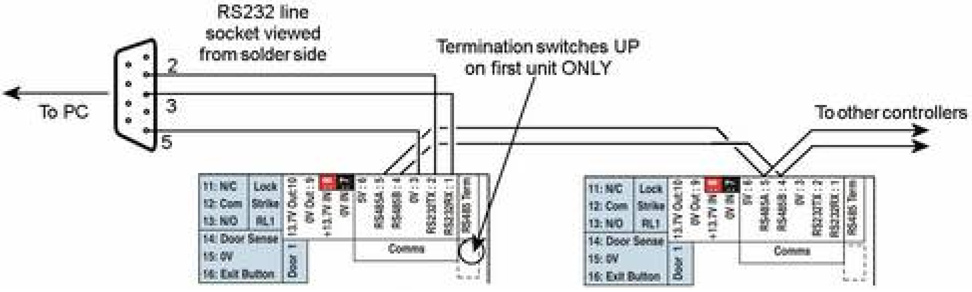


Figure 10 RS232 communication: first controller within 15m of PC

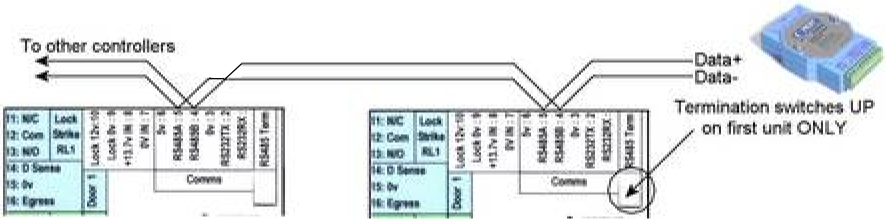


Figure 11 RS232 communication: first controller more than 15m from PC

Connection via USB

For USB connection use TDSi's USB to RS485 converter, part number 5012-0017.

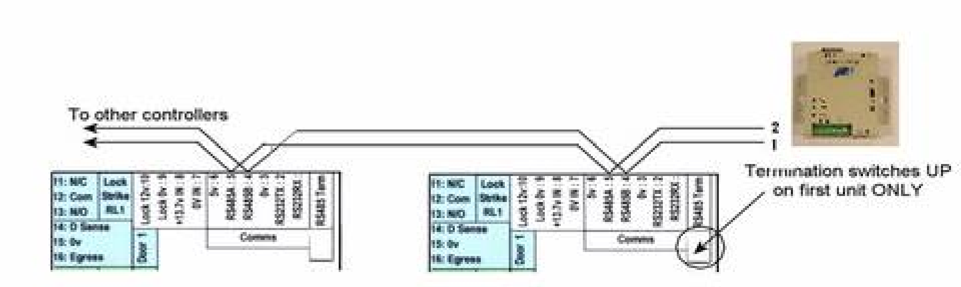


Figure 12 MICROgarde network using USB-RS485 converter

TCP/IP Ethernet

You can also connect a MICROgarde to the administration PC via a TCP/IP ethernet connection.

If you have not already done so, install TDSi's TCP/IP module (Part No. 5002-1812) as described on page 21 (alternatively other I/P converters such as the Lantronix UDS1100 can be used – refer to the documentation supplied with the I/P converter).

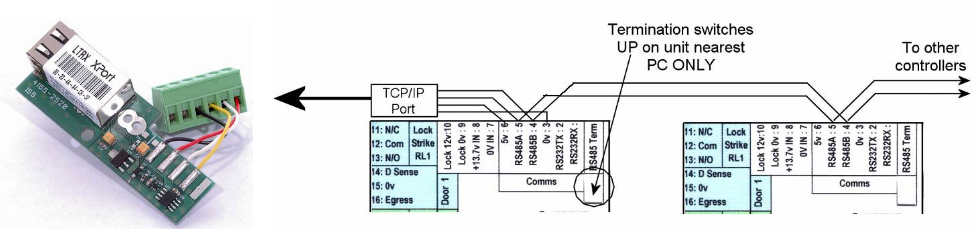


Figure 13 Ethernet communication (a) TCP/IP module, (b) connections to MICROgarde unit

Make a note of the MAC address to help with the MICROgarde software controller set up.

Connect the TCP/IP port to the PC's network port using a cross over Ethernet cable, or using a standard Ethernet patch cable into a network point.

2.4.7 MICROgarde Configuration

When you have completed the physical installation and connected the MICROgarde to readers, switches and other devices, there are four further tasks to complete the configuration of the unit:

- Set the rotary switch
- Make a note of the unit's unique software identification code (UID).
- Fit the tamper spring.
- Enable the onboard battery.

Rotary Dial switch

All MICROgarde units must have a unique number. The first 8 units must be set to addresses 1-8 and subsequent units set to position 9 which indicates that the UID of the controller will be used for addressing purposes. The software will assign a unique unit number for the additional controllers.

Make note of the Unit numbers given to your controllers to help in MICROgarde software set up.

UID

The UID is a unique number and should be noted for Software identification of the unit. Using EXgarde software you will be required to type this UID in. A MICROgarde 1 has a UID starting with 6, "6-xxx-xxx-xxx" and a MICROgarde 2 has a UID starting with 5, "5-xxx-xxx-xxx".

Tamper spring

The tamper spring should be slotted onto the tamper spring switch SW1 located near the Battery of the main PCB.

Battery

When you have completed installation and connection, it is essential that you remove the battery tab. This enables the onboard memory, allowing the unit to store all information (for example, access card details) should the unit lose power.

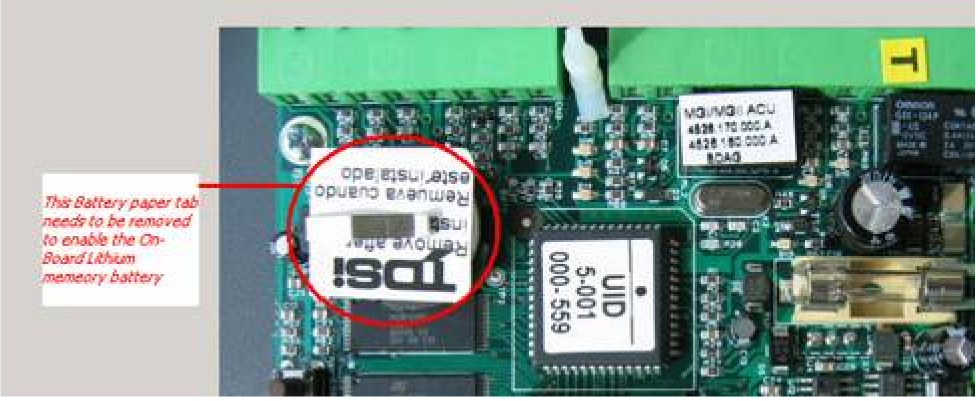

This Battery paper tab needs to be removed to enable the On-Board Lithium memeory battery
Remueva cuando este instalado
Remove after inst
TDSi
UID
5-001
000-559
MG/MG ACU
T

Figure 14   Enabling the onboard battery

2.5 Inputs

A MICROgarde input is used to sense the state of a switch. An Input comprises of two connections, which allows either an open circuit between the 2 connection points or a closed circuit. The normal state for a MICROgarde input is “open”; by shorting the input across the two connections, MICROgarde detects the change.

When the controller is configured to monitor and activate a door, two inputs are assigned:

- **Egress (Push to Exit) switch**
  If the egress connections are shorted the door is opened.
- **Door sense switch**
  Monitors the open or closed state of the door (the polarity of this switch can be programmed).

If these inputs are not assigned to their normal function you can use them for other functions such as controlling a relay: the input acts as a switch to trigger the relay.

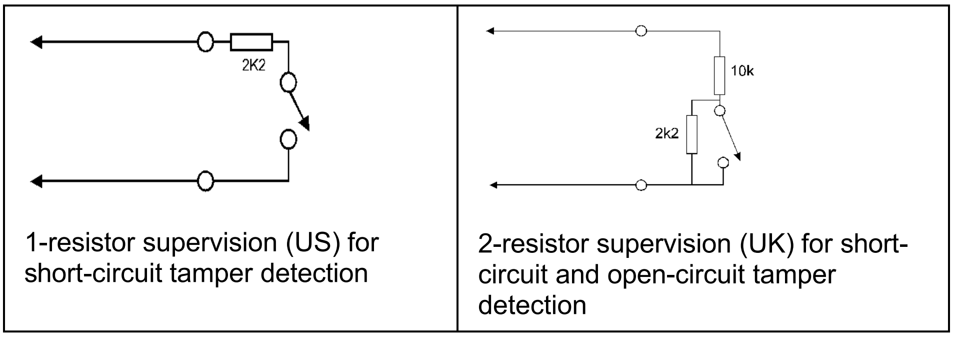
Inputs also can be activated by other devices e.g. Passive InfraRed sensors (PIRs).

Table 3 MICROgarde input connections

MICROgarde connection	Normal use	Alternative use
Connection 14 input 1	Door 1 Door sense	Spare Input 1 (if not door 1 defined)
Connection 15 input 1 and 2 ground	0V for Door 1 door sense and egress	0V
Connection 16 input 2	Door 1 egress	Spare Input 2 (if not door 1 defined)
Connection 20 input 3	Door 2 Door sense (MG2 only)	Spare Input 3 (if not door 2 defined)
Connection 21 input 3 and 4 ground	0V for Door 2 door sense and egress	0V
Connection 22 input 4	Door 2 egress (MG2 only)	Spare Input 4 (if not door 2 defined)

Supervised use

You can configure inputs for non-supervised or supervised (tamper detection) use. as shown below.



1-resistor supervision (US) for short-circuit tamper detection

2-resistor supervision (UK) for short-circuit and open-circuit tamper detection

Figure 15 Tamper-detection input configurations

2.6 Relays

Relays are often referred to as Outputs. They internally comprise an armature that flips from one connection to another. This creates either a closed circuit or an open circuit.

Applying external power (relays do not provide power themselves) via the relay then applies power from a PSU to other devices, e.g. a lock.

MICROgarde's two relays are dry-contact changeover type, rated at 30V, 2 A. Connect the lock to common and either N/C or N/O as described in *Lock supply*.

Devices which have inductive loads (i.e. anything with a coil, such as a secondary relay, bell or motor) must be fitted with suppression at the device. If in doubt, fit a suppressor. A DC device can be fitted with a diode (IN4003 or equivalent) as supplied with the MICROgarde. The suppressor must be fitted at the coiled component terminal (secondary relay, bell, motor, or lock), and not at the Controller circuit board terminal.

Table 4 MICROgarde relay connections

MICROgarde connection	Normal use	Alternative use
Connection 11 Relay 1 N/C Normally Closed	Lock Strike Door 1	Spare Relay 1 if Door 1 not defined
Connection 12 Relay 1 Common	Lock Strike Door 1	Spare Relay 1 if Door 1 not defined
Connection 13 Relay 1 N/O Normally Open	Lock Strike Door 1	Spare Relay 1 if Door 1 not defined
Connection 17 Relay 2 N/C Normally Closed	Lock Strike 2 (MG2 only)	Spare Relay 2 if Door 2 not defined
Connection 18 Relay 2 Common	Lock Strike 2 Common	Spare Relay 2 if Door 2 not defined
Connection 19 Relay 2 N/O Normally Open	Lock Strike 2 (MG2 only)	Spare Relay 2 if Door 2 not defined

2.7 Installing an Input/Output Module

You can add an I/O module to the PSU and non-PSU versions of the MICROgarde.

- **MICROgarde PSU version**: the input/output module comes with 3 self-tapping screws and 3 spacers for the metal cased MICROgarde. Fit these 3 screws through the I/O board and then screw on the plastic spacers provided, before fitting and screwing to the chassis.
- **MICROgarde non PSU version**: the I/O module has a white plastic cover but a metal chassis that has metal spacers already welded in position for the I/O board. Use the 3 x standard M3 screws that are provided.

To fit the module:

1. Remove the connection label from controller.
2. Fit the I/O Module using 3 screws (labelled "1" in the picture).
3. Fit the ribbon cable (labelled "2" in picture).
   The red wire of the ribbon cable should be adjacent to the tamper switch SW1.
4. Re-fit the connection label.

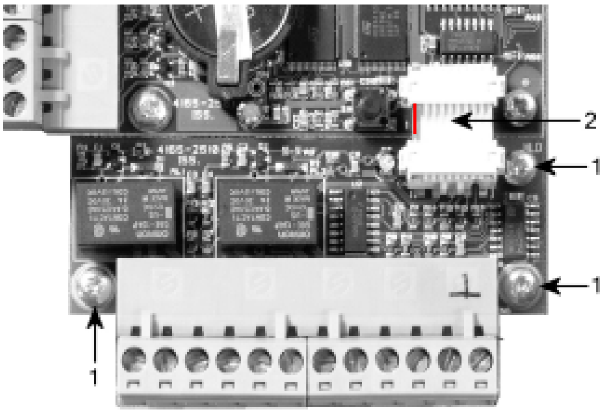


Figure 16 Installing an I/O module

Software Configuration

Install the I/O before auto detecting the MICROgarde controller (see page 36). The software then auto detects the I/O module.

2.8 Installing a TCP/IP Module

The MICROgarde TCP/IP module can be connected to 100Mb or 10Mb networks. In order to fully satisfy EU requirements for EMC and RFI, we recommend that this product only be connected to a 10Mb network port. On a 100Mb network, we recommend connection via a hub that is limited to 10Mb.

2.8.1 MICROgarde without PSU

The IP module connects to the top edge of main board (see below).

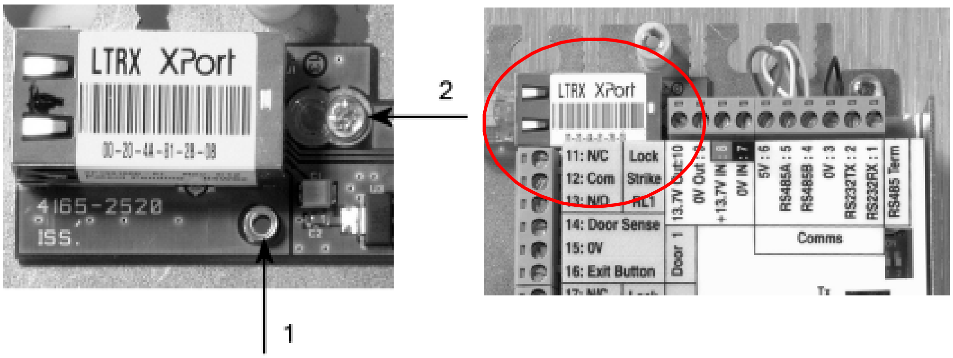


Figure 17 Installing a TCP/IP module to a MICROgarde without PSU

1. Remove the connection label from the controller, remove the Comms 6 pin connector (1-6), and temporarily remove power 4 pin connector (7-10). Remove 4 screws securing the controller to the metal plate and lift the controller away from the metal plate
2. Position the TCP/IP module over the pillar (labelled "1" in figure 2)
3. Fit the module to the plate with the screw provided (labelled "2" in figure 2)
4. Re-attach the main board to the metal plate and re-fit connection label
5. Connect the TCP/IP module to controller using the pre-wired connector provided.

Table 5 TCP/IP connector

Colour	Pin	Label
Red	6	+5V
White	5	RS485A
Yellow	4	RS485B
Black	3	0V

6. Set the RS485 termination switches to the upper position; i.e. ON, at this MICROgarde controller only: any other controller must have the RS485 termination switches set to OFF).

2.8.2 MICROgarde with PSU

The IP module connects to the right edge of the main board (see Figure 18a).

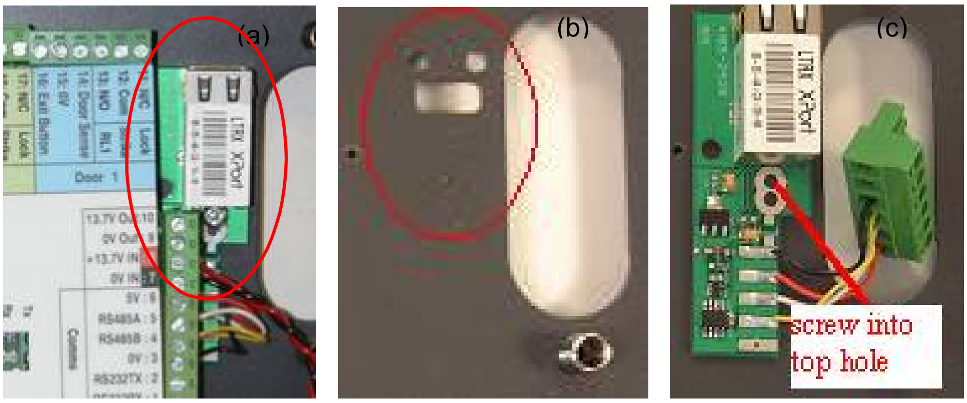


Figure 18 Installing a TCP/IP module to a MICROgarde with PSU

1. Remove the green COMMS 6 pin connector (1-6), and temporarily remove power 4 pin connector (7-10).
2. At the back of the TCP/IP modules board, fit a black stud over each of the two holes in the chassis (Figure 18b) situated on the right of the main board.
3. Position the module onto the chassis and secure with the self-tapping screw provided into the upper of the 2 holes (see Figure 18c). The module sits securely and flat onto the chassis.
4. Connect the TCP/IP module to the controller using the pre-wired connector provided (see Table 5).
5. Reconnect the power 4 pin connector (7-10).
6. Set the RS485 termination switches to the upper position; i.e. ON, at this MICROgarde controller only: any other controller must have the RS485 termination switches set to OFF).

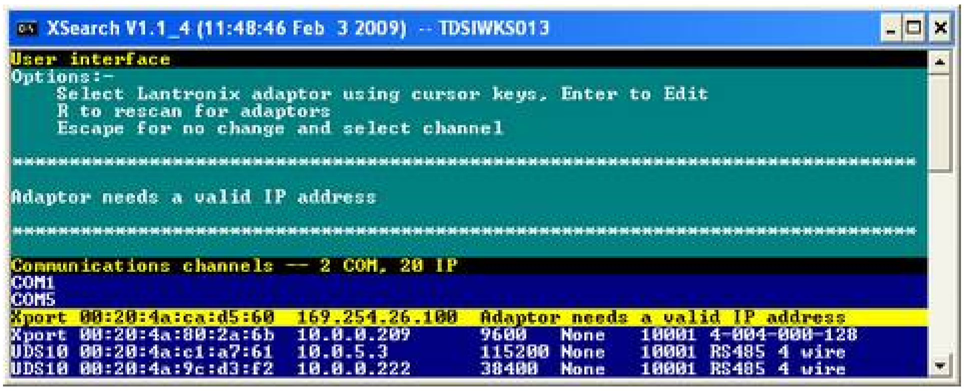
2.8.3 Software Setup

MICROgarde software assigns an I/P address automatically using the MAC Address of the XPORT TCP/IP module. You should not need to proceed with the following unless you encounter communication problems between the MICROgarde administration PC and the controller.

This normally occurs if you connect a TCP/IP module directly to an existing powered network. The network then assigns a “temporary” IP address to the TCP/IP module. It is essential that you “fix” a permanent I/P address. Otherwise, on each occasion there is a power loss or a network change, a new temporary I/P address might be assigned by the network. This would disrupt the MICROgarde controller’s communication with its administration PC.

Manually correcting the IP address

1. Install the TCP/IP module according to the previous section.
2. Install the XSEARCH software utility. This can be found in the *Extras/Toolkit/xsearch* folder of your software CD. Simply copy and paste the program to a convenient folder on the PC.
3. Power up the MICROgarde controller.
4. Connect the MICROgarde controller to your network. Ideally, use a crossover cable from your PC direct to the MICROgarde XPort TCP/IP module.
5. After several minutes, the Xport TCP/IP module will be auto assigned by the network to a “temporary” I/P address.
6. Run the XSEARCH utility program. Ensure no other software communications applications are running on the PC.
7. XSEARCH searches the communications ports and lists all IP devices (see below).

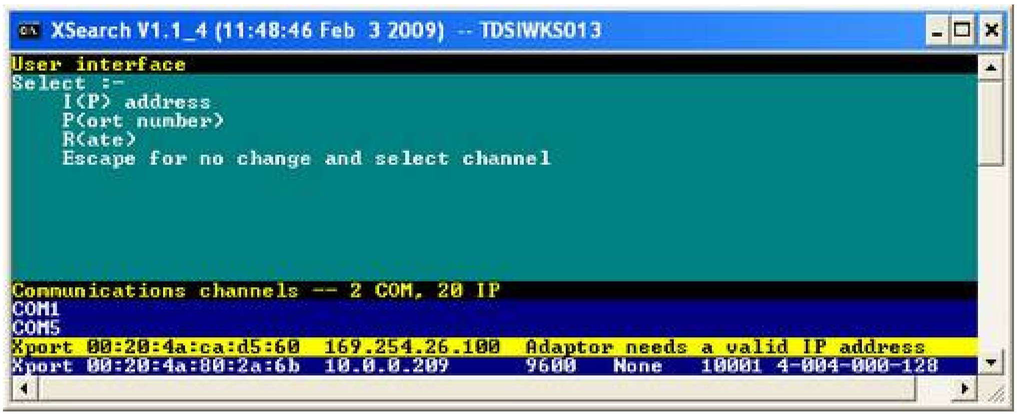


```
User interface
Options:-
    Select Lantronix adaptor using cursor keys, Enter to Edit
    R to rescan for adaptors
    Escape for no change and select channel

******************************************************************************

Adaptor needs a valid IP address

******************************************************************************

Communications channels -- 2 COM, 20 IP
COM1
COM5
Xport 00:20:4a:ca:d5:60  169.254.26.100  Adaptor needs a valid IP address
Xport 00:20:4a:80:2a:6b  10.0.0.209      9600   None   10001 4-004-000-128
UDS10 00:20:4a:c1:a7:61  10.0.5.3        115200 None   10001 RS485 4 wire
UDS10 00:20:4a:9c:d3:f2  10.0.0.222      38400  None   10001 RS485 4 wire
```

Figure 19 XSEARCH identifies a TCP/IP module with an invalid IP address

8. Locate the MICROgarde’s XPort TCP/IP module. You can identify this by looking for its MAC address number as written on the module, e.g. “00:20:4a:ca:d5:60”. It can also be identified by the statement: “*Adapter needs a valid IP address*”.
9. Use the up and down arrows on the PC keyboard to highlight the Xport TCP/IP unit. Press the ENTER key.

10. Press the letter “I” and then type in the new IP address (see below). This must be valid for the network you are using.



```
User interface
Select :-
    I(P) address
    P(ort number)
    R(ate)
    Escape for no change and select channel




Communications channels -- 2 COM, 20 IP
COM1
COM5
Xport 00:20:4a:ca:d5:60  169.254.26.100  Adaptor needs a valid IP address
Xport 00:20:4a:80:2a:6b  10.0.0.209      9600    None    10001 4-004-000-128
```

Figure 20 Entering an IP address using XSEARCH

11. Press the ENTER key to save the setting and return to the main screen.

12. XSEARCH should now show your Xport unit with the MAC address, the correct I/P address and the UID number of the MICROgarde unit.

Troubleshooting TCP/IP

Some of the common problems are listed below. If you continue to have problems then other software tools such as Lantronix Device Installer and Telnet are other methods which may help you.

For further help, contact TDSi Support or refer to other TDSi I/P documents.

What is the module’s default IP address?

A new XPort TCP/IP is not assigned an I/P address, so the default is 0.0.0.0.

What is a temporary IP address?

When you connect the module to a network or a PC using a crossover cable the I/P address is of the form: 169.254.*.*. This is a temporary address awaiting a valid “fixed” I/P address.

Unable to see module in XSEARCH

When first searching for the XPort TCP/IP module you may not see the device if its IP address is outside the range of the PC. Check that the PC has a range that can detect the temporary IP address of the module. Try a laptop or PC using just a crossover cable, and assign the IP address of the PC to be close to 169.254.0.0 with a subnet of 255.0.0.0 and no gateway.

Unable to ‘see’ module on laptop after fixing for network

Once you have changed the module’s I/P address for a network you may not see the unit on your laptop if it has been changed to a number out of the range of the laptop’s I/P address.

2.9 Final Installation Checks

The following tests will confirm that the controller, reader(s), lock(s) and exit buttons are correctly connected. Testing any door sensors requires the software to be running and will be checked as part of the software setup (see page 38).

> **Note.** If MICROgarde PC software is already running, disconnect the communications to the MICROgarde controller by unplugging the 6-way connector.

1. Set the rotary switch of the unit to 0 (see below).

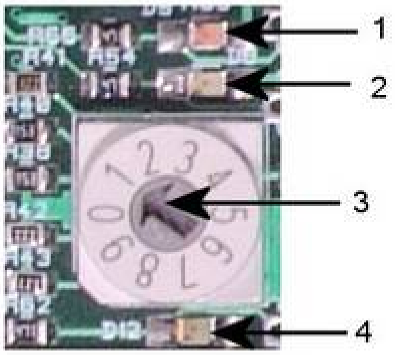


Figure 21 System checks and rotary dial switch setting

2. Power up the unit.
3. Set the rotary switch to the correct address: 1-8 or 9:
   - With MICROgarde software, use 1-8 for the first eight units in a network. Set additional units to 9.
   - With EXgarde PRO set all units to 9.
4. Check that the 5V On light (see 4 in Figure 21) illuminates and that the red LED on each reader flashes continuously (2 flashes per second).
5. Present a card to any reader. The flashing rate of the red LED (on all readers) changes to once every 2 seconds.
6. Put the unit into "*installer mode*":
   a. Carry out a hardware reset (see page 26).
   b. Press the tamper switch down for 5 seconds.
   c. Release the tamper switch for 5 seconds.
   d. Press the tamper switch again down for 5 seconds.
   e. Release the tamper switch again for 5 seconds.
   f. Press the tamper switch down again for 5 seconds.
   g. Release the tamper switch again for 5 seconds.

   During this action the relay 1 will activate for 5 seconds and D13 red LED will light up for 5 seconds.
7. Present the card again to any reader:
   - Both Relays 1 and 2 operate for 5 seconds. Any locks connected to these relays are unlocked for 5 seconds.

  - The Relay 1 and 2 red LED indicators (D13 and D14) illuminate for 5 seconds (regardless of the number of doors the controller will be controlling).

8. Press any Exit button. The associated lock is unlocked for 5 seconds.
9. Tests are now complete. Change the rotary switch to the required number.
10. Re-connect the communications link if necessary. If MICROgarde PC software is running, the Tx and Rx lights will start flashing rapidly.
11. Exit installer mode by one of the following actions:
    - Shutdown and restart the software.
    - Validate a card using the software (see page 40)
    - Perform a hardware reset (see below).
12. In Normal operation mode:
    - The Reader LED flashes once every two seconds.
    - When a “non-valid” card is presented to a reader the reader LED lights up red for 5 seconds.
    - When a valid card is presented to a reader the reader LED lights up green for 5 seconds and the corresponding lock relay will trigger.

2.9.1 Hardware Reset

To perform a hardware reset:

1. Turn off the MICROgarde unit.
2. Set the dial switch to zero (see Figure 21).
3. Switch the MICROgarde unit on.
4. Wait 20 seconds (watch for 4 green flashes on LED D8 followed by a pause and then 8 or 9 more green flashes).
5. Turn the dial back to the required unit number (1 to 8 or dial 9 for UID which selects next available unit number).

After the hardware reset:

- The unit’s memory is cleared.
- The LED on any fitted reader will flash red, twice a second.
- The first time you present a card to a reader it sets the reader into its ready mode and its LED flashes once every 2 seconds. The second time you present the card, the reader’s LED illuminates fully to indicate “*access denied*”.

The unit is ready to receive a reset and upload from the software and card validation.

3. Software Installation

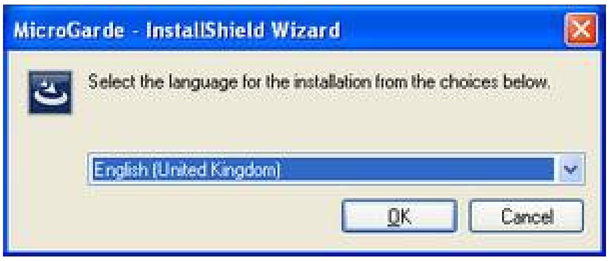
3.1 Preinstallation Checks

Before installing the MICROgarde CD:

1. Ensure that your computer meets the required specification:
   - Workstation grade architecture
   - 32-bit operating system
   - 32-bit/64-bit processors – Intel Core i5 Sandybridge or above
   - Virtual PC environment not supported
   - 4GB RAM
   - 100MB-BaseT network interface or above
2. Ensure that you are logged on to the PC as a user with full Administrator rights. Close any applications that are running.
3. Enable **File and Printer Sharing**:
   Choose **Start > Control Panel > Network**.
   Right-click **Local Area Connection** and select **Properties**.
   Look for *File and Printer Sharing for Microsoft networks* - if this is not in the list then click on **Install**; if it is in the list then ensure it is selected.

3.2 Installation

1. Insert the CD into a CD-ROM drive:
2. Select the language you require.


MicroGarde - InstallShield Wizard

Select the language for the installation from the choices below.

English (United Kingdom)

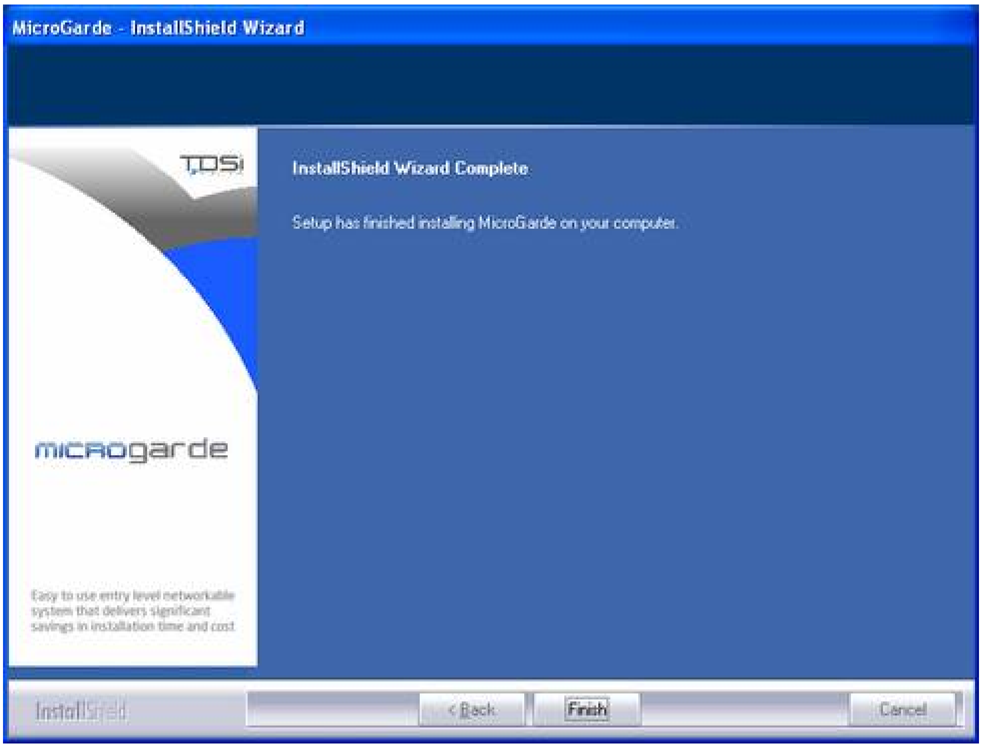
Figure 22 Selecting the language

3. Your Computer may be missing some software components required by MICROgarde software. If this occurs, click on the **Install** button and the installer will attempt to install the components for you.

Note. The installation of some components may require a restart of the PC. After this, the installation of MICROgarde will resume. You also may need to install several components.

4. Follow the on-screen instructions until the *MICROgarde Installation Complete* screen is displayed.

5. Click on the **OK** button to continue.



MicroGarde - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing MicroGarde on your computer.

TDSi
microgarde
Easy to use entry level networkable system that delivers significant savings in installation time and cost
InstallShield
< Back
Finish
Cancel

Figure 23 Finishing the software installation

6. Click on the **Finish** button.

7. Restart the computer.

4. Getting Started

This section provides an introduction to MICROgarde Explorer and explains how to set up a controller system for the first time. More detailed information and advanced features are described in the next chapter.

Note. While it is possible to set up the system without any controllers connected, we recommend that you have at least one connected and powered up in order to confirm that the software is correctly set up. If you have more than one controller set up, then each has a unique unit number set using its rotary switch. If you are using TCP/IP communications, you should also have noted the "Mac" address of the controller - this is a number in the format 00-20-4A-81-28-09 printed on a label close to the communications cable (see Figure 1).

To get started:

1. Run MICROgarde Explorer.
2. Log in using the default Admin operator account.
3. Familiarize yourself with MICROgarde Explorer.
4. Change the Admin password and set up your own Operator account.
5. Run the System Settings Wizard.
6. Add your Controllers.
7. Configure the Controllers.
8. Add one or more cards and card holders and test the system.

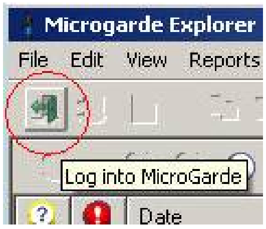
4.1 Starting MICROgarde Explorer

To run the MICROgarde software:

- Double click on the MICROgarde icon on your desktop, or
- Choose **Start > All Programs > MICROgarde > MICROgarde**

MICROgarde Explorer is displayed.

4.2 Logging In



To log in to the MICROgarde software:

1. Choose **File > Log into MICROgarde** or click on the Login button on the toolbar.
2. The login screen is displayed with the username set to *Admin*. The Admin account has a default password of “1234” but on the first occasion that you log in you can immediately change this password. Type in a new password less than 10 characters long (remember it is case-sensitive).

Note. PLEASE REMEMBER THE PASSWORD, for your security, we have designed the system so that there is no "back door" into the database.

3. Click on **OK**.

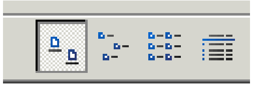
4.3 MICROgarde Explorer

The main features of MICROgarde Explorer are shown in Figure 24.

1. **Menu and tool bar**.
   Provides access to all MICROgarde Explorer commands including reporting options.

2. **Shortcut bar**
   Features links to the main components of the MICROgarde system: Card Holders, Cards, Access Levels, Controllers, Doors, Readers, Inputs, Relays.

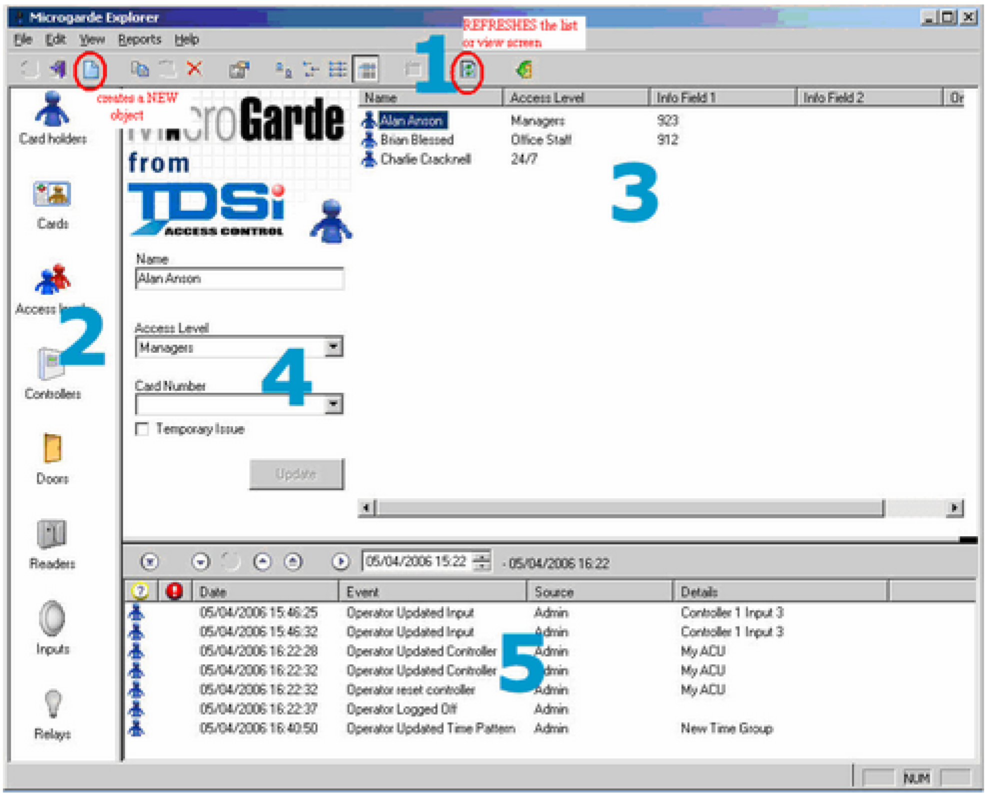
3. **Display area**
   Lists all registered components within the selected category. For example, if you select *Card Holders* in the Shortcut bar, all the registered card holders will be listed here.



   You can change the way objects are displayed by using the View icons in the toolbar: (Left to right: Large icons, small icons, tile, detail)
   Select an object in the display area to display editable properties in the Quick Data Entry area.

4. **Quick Data Entry area**
   Allows you to edit some of the general properties of the selected object. For example, if you have selected a Card holder in the display area, you may edit the Card Holder's access level in the Quick Data Entry area.

5. **Event window**
   View system events for any period within the previous 45 days. All new events appear here automatically unless you have browsed to older events. Events remain in the database for 45 days after which they are automatically deleted.



Name	Access Level	Info Field 1	Info Field 2	Or
Alan Anson	Managers	923		
Brian Blessed	Office Staff	912		
Charlie Cracknell	24/7			

Name: Alan Anson

Access Level: Managers

Card Number:

□ Temporary Issue

05/04/2006 15:22 - 05/04/2006 16:22

Date	Event	Source	Details
05/04/2006 15:46:25	Operator Updated Input	Admin	Controller 1 Input 3
05/04/2006 15:46:32	Operator Updated Input	Admin	Controller 1 Input 3
05/04/2006 16:22:28	Operator Updated Controller	Admin	My ACU
05/04/2006 16:22:32	Operator Updated Controller	Admin	My ACU
05/04/2006 16:22:32	Operator reset controller	Admin	My ACU
05/04/2006 16:22:37	Operator Logged Off	Admin	
05/04/2006 16:40:50	Operator Updated Time Pattern	Admin	New Time Group

Figure 24 MICROgarde Explorer

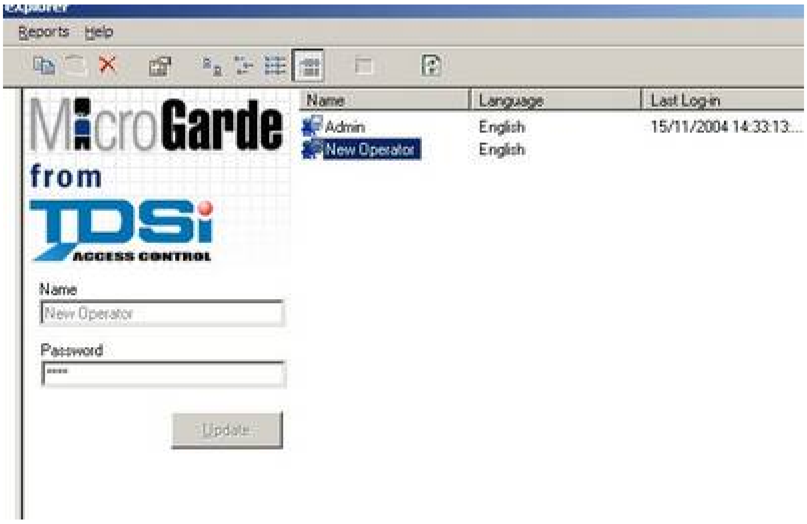
4.4 Creating an Operator Account

Having changed the Admin password, write it down and lock it away securely. We recommend that you now create your own operator account and do not use the Admin operator account again unless you have forgotten the password for your own operator account.

Note. If you did not change the password when you first logged in, you can do so by choosing **View > Operators**; click on **Admin** in MICROgarde Explorer. See page 77 for details.

To create a new Operator account:

1. Select **View > Operators**.
2. Click on the **New** button.
3. Type in the new Operator name and password.
4. Confirm the password.



Name: New Operator

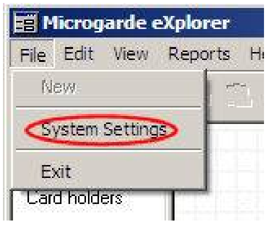
Password: ****

Name	Language	Last Log-in
Admin	English	15/11/2004 14:33:13...
New Operator	English	

Figure 25 Adding a new Operator account

5. By default, a new operator account has full access rights. To check that this is the case, see page 78.
6. Close MICROgarde Explorer, re-start it and log back in using the new operator account.

4.5 The System Settings Wizard



The System Settings wizard appears automatically when you run MICROgarde Explorer for the first time and until you have carried out the setup process.

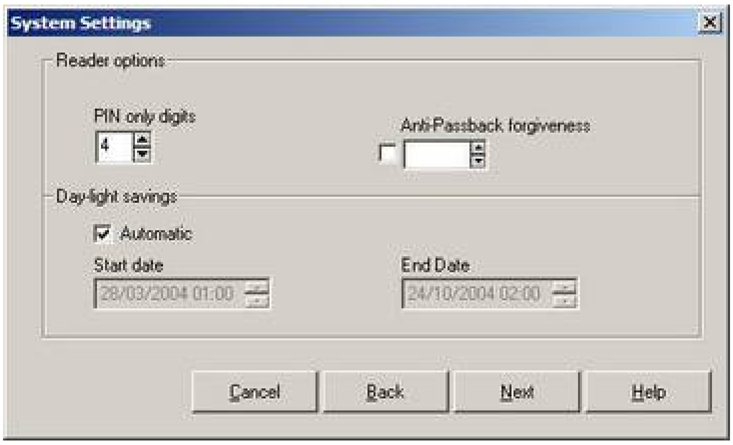
You can also display the System Settings wizard by choosing **File > System Settings**.

4.5.1 Reader Options

There is no need to change any information in this screen. However, these settings affect the whole system:

- **PIN-only digits**
  Only applicable if you have one or more keypads installed AND want to allow access (for some or all people) without the use of a card or fob, simply by entering a sequence of numbers at a keypad.
- **Anti-passback forgiveness**
  Only applicable if you enable anti-passback at one or more doors. Anti-passback is designed to make it difficult for two people to gain access using the same card, by preventing re-use of a card within a set number of minutes. This "forgiveness" setting allows you to have all cards automatically cleared at a set time of day for access.
- **Day-light savings**
  We recommend you leave this set to automatic. The controllers will be programmed with the appropriate dates according to the regional settings in your computer.

Click on **Next** to continue.



Reader options

PIN only digits: 4

Anti-Passback forgiveness: ☐

Day-light savings

☑ Automatic

Start date: 28/03/2004 01:00

End Date: 24/10/2004 02:00

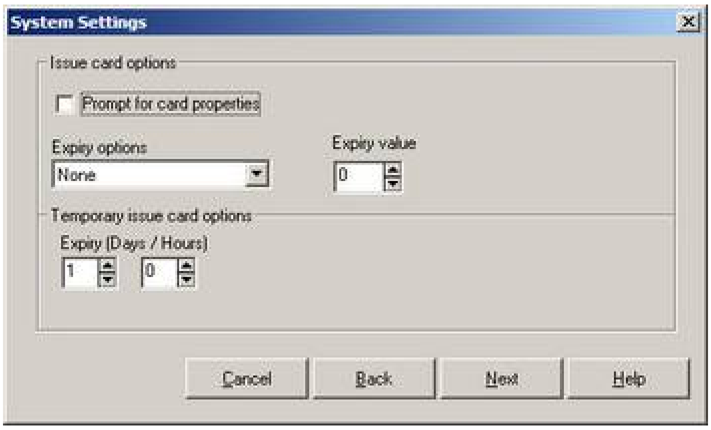
Figure 26 System Settings – Reader Options

4.5.2 Card Options

There is no need to change any *Issue Card Options*. However, these settings affect the whole system:

- **Issue Card options**
  Select the *Prompt for card properties* check box, if you want to be prompted for an expiry date each time you issue a card. Otherwise, if you leave the check box clear, each card you add will have the Expiry options set automatically to the values shown here.
- **Temporary issue card options**
  When you issue a card to a Card Holder, and set the Temporary Issue option (see page 40), the card will expire after the length of time set here.

Click on **Next** to continue.



System Settings

Issue card options

□ Prompt for card properties

Expiry options: None

Expiry value: 0

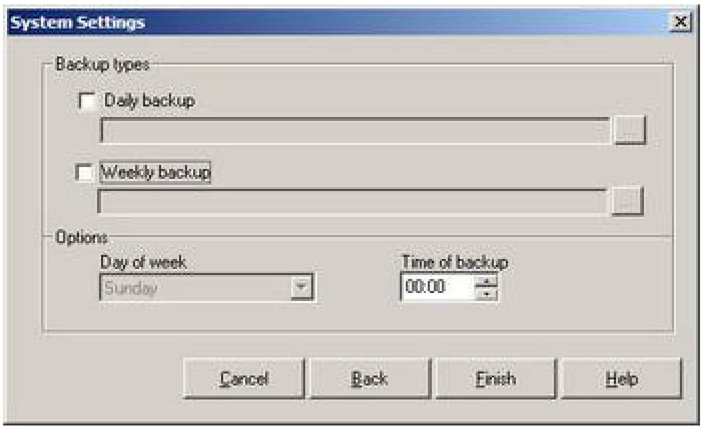
Temporary issue card options

Expiry (Days / Hours): 1 / 0

Figure 27 System Settings – Card Options

4.5.3 Backup

Use this screen to specify how MICROgarde creates data backups for your data. Backing up your data is vital: if your computer experiences a hard-disk failure and you have no backup then you will have to re-enter all user and card data.



System Settings

Backup types

□ Daily backup

□ Weekly backup

Options

Day of week: Sunday

Time of backup: 00:00

Figure 28 System Settings – Backup options

Ideally, you should enable both Daily and Weekly backups. Choose a backup location either on a separate disk in your computer or on a mapped network drive on another computer. Backups are recorded in the Events Log.

Note. A single hard disk formatted with two partitions can lose both partitions at once if the disk fails, so simply backing up to a second partition is not a secure option.

The backup file (given a .bak extension) is saved in the specified folder.

Click on **Finish** to continue.

About backups

MICROgarde automatically runs a scheduled backup even if MICROgarde Explorer is not running. All that is necessary is that the MICROgarde computer is switched on: it doesn't matter whether anyone is "logged on" to the computer.

Daily backups are automatically deleted when more than 7 days old, and Weekly backups after 4 weeks. After operating MICROgarde for a month, you should only have 10 backups in total. If a problem is not discovered until several days after it has occurred (e.g. data corruption, or accidental data deletion by an operator) then you are likely to be able to go back to a backup that was created before the problem existed.

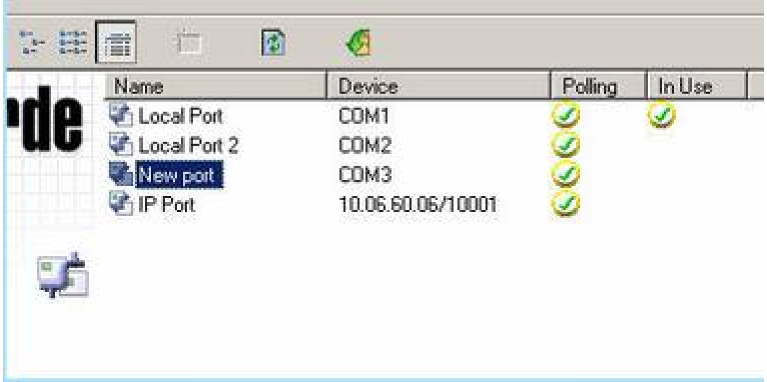
Restoring data from a backup basically involves replacing ALL existing data with the backed up data. All changes made between the backup date and the current date will be lost.

If you need to restore a backup, please refer to page 93.

4.5.4 Communication Ports

Each MICROgarde controller that is connected to the administration PC does so through either a serial port or TCP/IP connection. To configure the ports, choose **View > Ports**.

MICROgarde Explorer displays a summary of all of the ports that are configured in the system as shown below.



Name	Device	Polling	In Use
Local Port	COM1	✓	✓
Local Port 2	COM2	✓	
New port	COM3	✓	
IP Port	10.06.60.06/10001	✓	

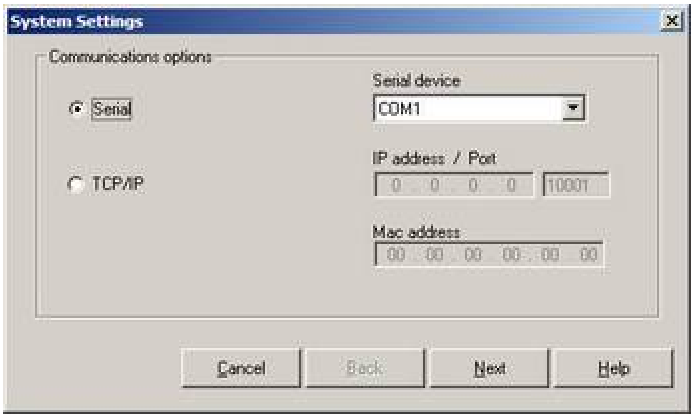
Figure 29 Viewing Ports

Adding a new port

To add a new port, right click in the window and select **New** from the context menu.

Configuring a Port

To configure a port, right click on it and select **Properties** from the context menu.



System Settings

Communications options

● Serial

○ TCP/IP

Serial device: COM1

IP address / Port: 0 . 0 . 0 . 0 / 10001

Mac address: 00 : 00 : 00 : 00 : 00 : 00

Figure 30 Configuring a port

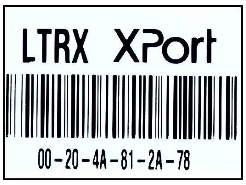
Serial

Choose this option if the controller connects to a serial port on the PC. Select the COM port from the *Serial device* dropdown list box.

TCP/IP

Choose this option if the controller connects to a TCP/IP (Ethernet) network port on the PC:

- If you are connecting using an existing network, contact your network administrator for a suitable IP address.
- If this is a direct Ethernet link between this computer and the controller, you will need to know (or set) the IP address for the computer, and then choose an address for the controller. For example 192.168.1.1 for the computer (subnet mask 255.255.255.0) and 192.168.1.2 for the controller.



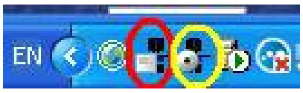
We recommend that you leave the Port set to 10001 for all TDSi controllers unless your network administrator tells you otherwise.

Enter the controller's unique *Mac address* exactly as it appears on the label (see left) close to where the Ethernet cable is plugged in to the controller.

When you have configured the port, click on **Next**.

4.6 Setting up a New Controller

4.6.1 Checking Communications

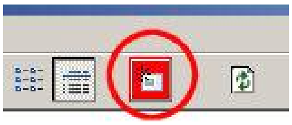


MICROgarde's communications software starts automatically and its icon appears in the Windows System Tray (see left – circled in red). In addition, you may see the icon circled in yellow, which indicates that the backup program is running.

If you see no icon, or the icon has a flashing red exclamation mark, then communication has not started (see the Troubleshooting guide on page 89).

Note. If you close the communications function, each controller will remain functioning, storing events until its internal buffer is full. At this point, the controller overwrites the oldest event (the default is 1,000 events per controller). Without the communications function, you will not be able to update controllers with any changes, new cards for example, or receive system events.

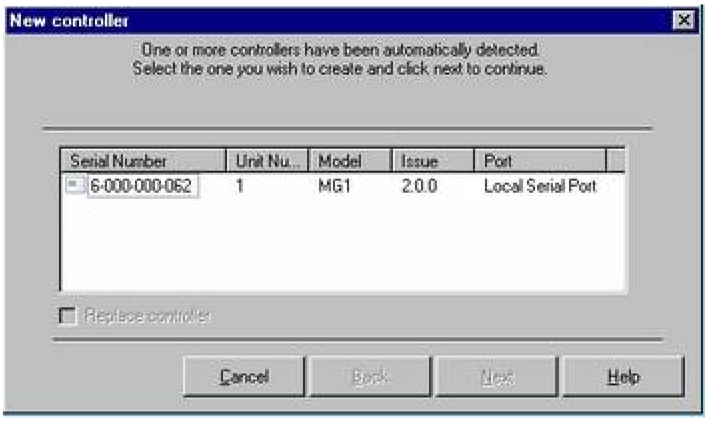
4.6.2 New Controllers



If the communications software has started normally AND you have at least one controller connected and powered up, then the "*New controller*" icon should be flashing on the MICROgarde Explorer toolbar. If the communications port is configured for TCP/IP, detection of the first unit may take up to a few minutes.

Note. If you know you have one unit connected, but the icon is still not flashing after a few minutes, the unit has not been detected (see the Troubleshooting guide on page 89).

Click on the flashing icon on the MICROgarde Explorer toolbar to view a list of all detected controllers.



New controller

One or more controllers have been automatically detected.
Select the one you wish to create and click next to continue.

Serial Number	Unit Nu...	Model	Issue	Port
6-000-000-062	1	MG1	2.0.0	Local Serial Port

□ Replace controller

Figure 31 Listing a new controller

To configure a new controller, select it by clicking on its **Serial Number UID** and then click on **Next**. The *New access control point* dialog box is displayed (see Figure 32).

Note. If there is a controller in the database with the same unit number and configuration (i.e. with or without an Input/Output module), you will be prompted to choose whether to replace it with the new controller.

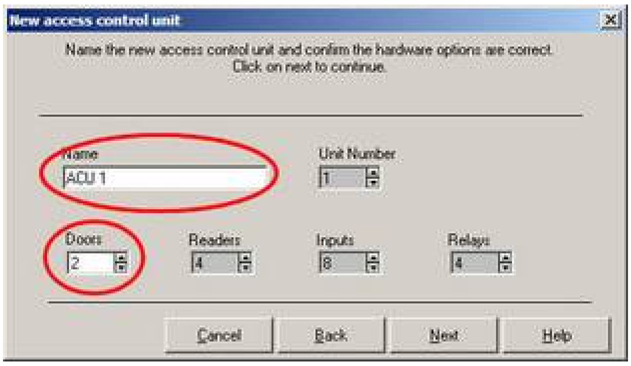
Defining controllers

The software displays the *New access control point* dialog box for each networked controller. It automatically detects the *Unit Number* and the numbers of installed *Readers*, *Inputs* and *Relays*. You can change:

- **Name**
  A unique name to identify the controller.
- **Doors**
  The number of doors this unit controls. It is important you select the correct number of doors here: the only way to change this is to delete and recreate the MICROgarde controller configuration.

Click on **Next**.

Repeat this configuration process for each controller in the system.



New access control unit

Name the new access control unit and confirm the hardware options are correct.
Click on next to continue.

Name: ACU 1
Unit Number: 1
Doors: 2
Readers: 4
Inputs: 8
Relays: 4

Figure 32 Defining the Controller name and door configuration

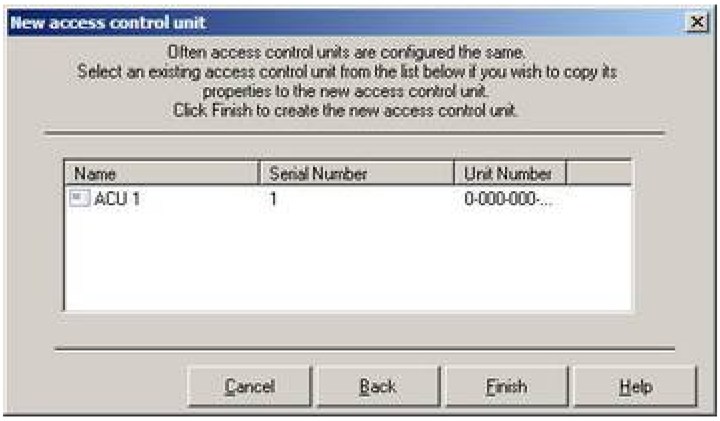
Note. During this process, MICROgarde Explorer may display events in the Event window. It is important that you complete this configuration process before attending to any events (see page 83).

Copying a configuration

You can apply the configuration of an existing controller to a new controller.

Select the controller that you want to use as the basis for configuring a new controller.

Click **Finish**.



New access control unit

Often access control units are configured the same.
Select an existing access control unit from the list below if you wish to copy its properties to the new access control unit.
Click Finish to create the new access control unit.

Name	Serial Number	Unit Number
ACU 1	1	0-000-000-...

Figure 33 Copying a configuration to other controllers

4.7 Configuring a Controller

To configure a controller:

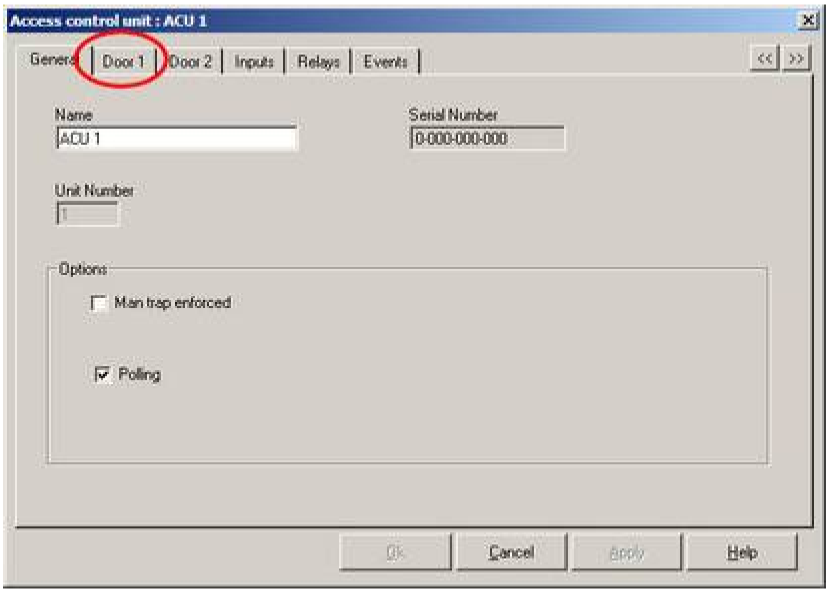
Click on **Controllers** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the installed controllers.

Either double-click on the controller's name or right-click on it and select **Properties** from the context menu.

The *General* page of the controller's properties is displayed (see Figure 34).

4.7.1 Name and Unit Number

Use the **General** page to change the name of the controller and, for larger systems with 9 or more controllers, to set the unit number.



Name: ACU 1

Serial Number: 0-000-000-000

Unit Number: 1

Options

□ Man trap enforced

☑ Polling

Figure 34 Controller properties: General page

The software reads the *Serial Number* from the controller and this cannot be changed.

The *Unit Number* is 'read only' if the MICROgarde dial switch has been set to positions 1-8. When set to position 9, the unit number (9 or greater) must be set here (see page 17).

Man trap enforced and *Polling* options are described on page 52.

Click on the **Door** tab to continue.

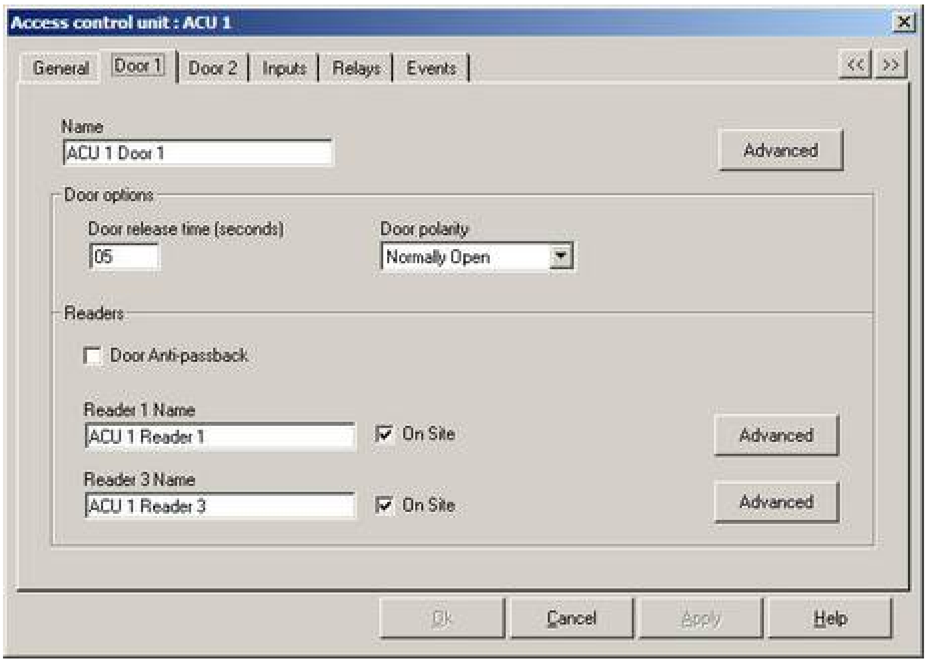
4.7.2 Door Configuration

Use the **Door 1** and **Door 2** pages to change the properties of doors and readers. The default settings allow you to quickly set up and test a system and you do not need to change anything at this stage. However, we recommend that you give the door and reader(s) identifiable names so that you can easily recognize them when they feature in the event list.

By default:

- Door lock polarity is set to *normally open.* If the door has a door sensor fitted, open and close the door and confirm that event messages appear in the right order - if not, you need to change the polarity to *normally closed*.
- When activated, a door remains open for five seconds.
- *Door antipassback* is disabled.

For more information about these and more advanced settings, see page 50.



Access control unit : ACU 1

Tabs: General, Door 1, Door 2, Inputs, Relays, Events

Name: ACU 1 Door 1

Door options

Door release time (seconds): 05

Door polarity: Normally Open

Readers

□ Door Anti-passback

Reader 1 Name: ACU 1 Reader 1 ☑ On Site

Reader 3 Name: ACU 1 Reader 3 ☑ On Site

Figure 35 Controller properties: Door page

The default reader names are derived by the software using the logic described in the following table.

Table 6 Reader naming convention

Reader	Reader number
Door 1, first reader	1
Door 1, second reader in a 2-door configuration (MG2 Unit Only) (i.e. Brown & White linked)	3
Door 1, second reader in a 1-door configuration (i.e. using pins 28 & 29)	2
Door 2, first reader (MG2 Unit Only)	2
Door 2, second reader (i.e. Brown & White linked) (MG2 Unit Only)	4

If you have other controllers and doors to configure, use the arrow keys in the top right corner of the dialog box to browse directly through their settings.

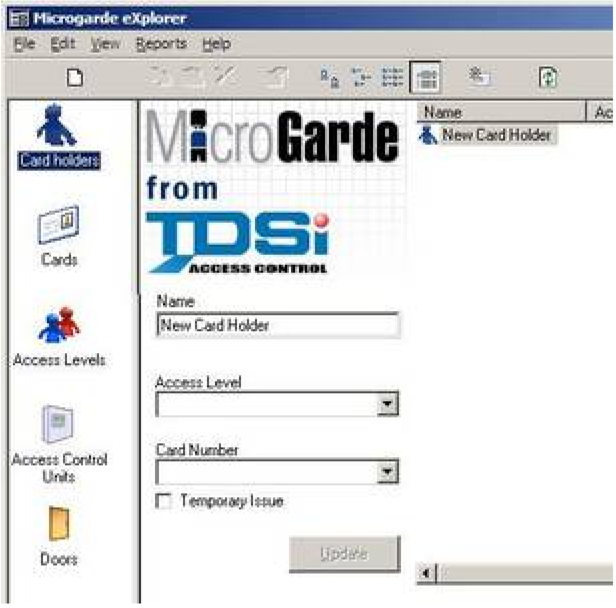
Click on **OK** to save any changes.

4.8 Adding a Card Holder

To add a card:

1. Click on **Card holders** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the names of current card holders (if any).
2. Either click on the **New** icon on the toolbar or select **File > New**.

   MICROgarde Explorer displays a form for adding details about a new card holder.



Name: New Card Holder

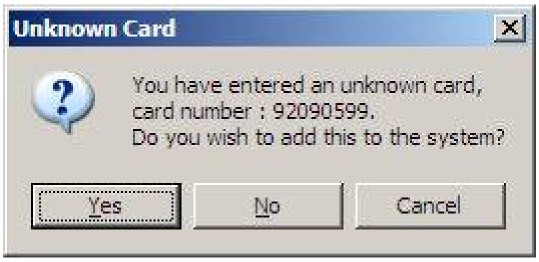
Access Level:

Card Number:

□ Temporary Issue

Figure 36 Listing card holders

3. Enter the name of the new Card Holder (up to 30 characters) by replacing the text: "New Card Holder"
4. Use the **Access Level** dropdown list box to select the default: "24/7". This allows access through every door, at all times, every day. You can create different access levels (see page 48).
5. In the **Card Number** field, type the number of card that you want to assign to the card holder. In regular use, when there are cards in the database, you can also use the drop-down list to choose an un-issued card.
6. Click the **Update** button and click **Yes** to the following question:



You have entered an unknown card,
card number : 92090599.
Do you wish to add this to the system?

Figure 37 Confirming a new card

7. Click **Update** again to save the details for this card holder

Test the card at a reader and confirm that the door is unlocked for 5 seconds.

5. Advanced Configuration

The previous chapter provides a quick overview of the key steps required to set up a new MICROgarde system. This chapter is a detailed reference guide to the various configuration options in MICROgarde. You can access the following through MICROgarde Explorer's shortcut toolbar:

- Card Holders
- Cards
- Access Levels
- Controllers
- Doors
- Readers
- Inputs
- Relays

The following configuration options are not available in the shortcut toolbar and must be accessed from the **View** menu:

- Operators
- Time Patterns
- Holidays

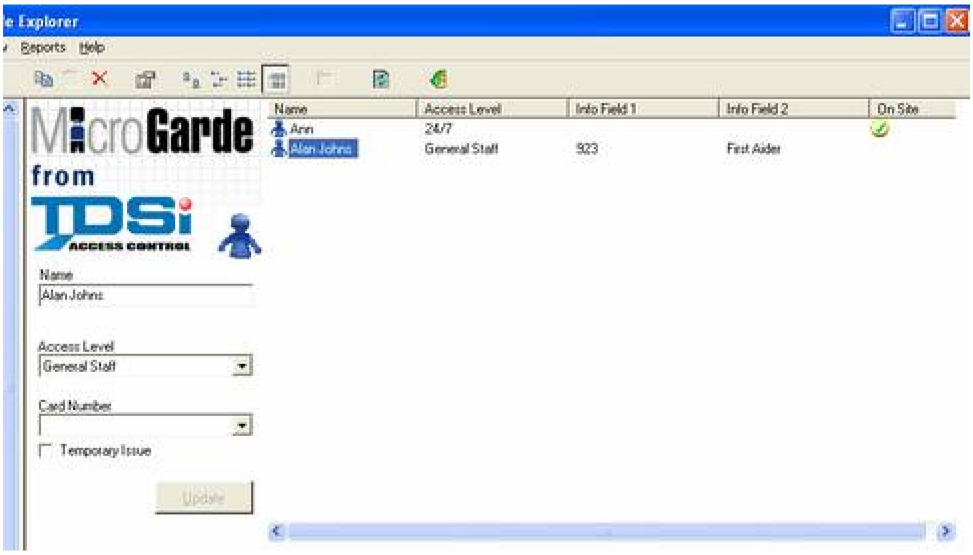
The final section of this chapter describes the management of events and event messages.

5.1 Card Holders

MICROgarde has capacity for up to 5000 cards, although each Card Holder can use multiple cards. Where a Card Holder has more than one card, each un-expired card will have exactly the same access rights, although different cards for a Card Holder can expire on different dates.

5.1.1 Viewing Card Holders

To display existing card holders, click on **Card Holders** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the defined card holders in the main display area.



Name	Access Level	Info Field 1	Info Field 2	On Site
Ann	24/7			✓
Alan Johns	General Staff	923	First Aider	

Name: Alan Johns

Access Level: General Staff

Card Number:

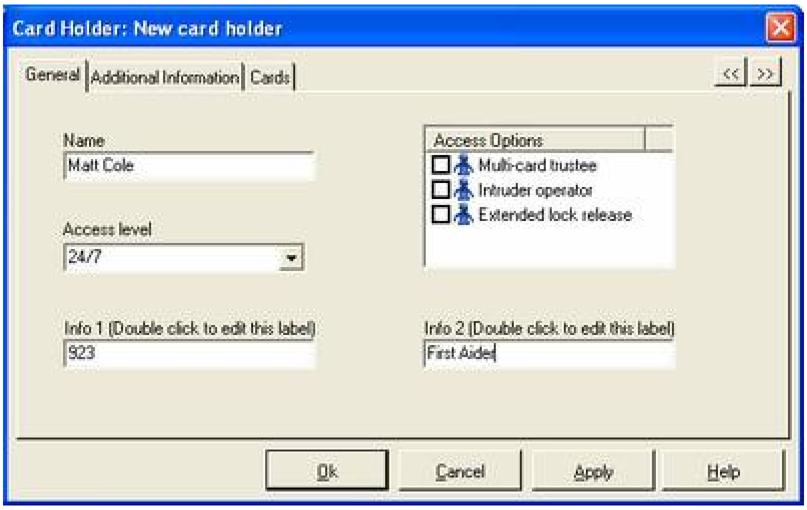
□ Temporary Issue

Figure 38 Listing Card Holders

To view the detailed properties of a card holder, double-click on their name or right-click on it and select **Properties** from the context menu.

The *General* page of the card holder's properties is then displayed (see below).

5.1.2 Card Holder Properties



Name
Matt Cole

Access level
24/7

Access Options
□ Multi-card trustee
□ Intruder operator
□ Extended lock release

Info 1 (Double click to edit this label)
923

Info 2 (Double click to edit this label)
First Aider

Figure 39 Card Holder properties: General page

- **Name**
  30 characters, must be unique
- **Access Level**
  The choice made here determines which doors, and at which times, this Card Holder can get through.
- **Access Options**
  The choice made here affects both Multi-card access and Intruder inhibit:
  - **Multi-card trustee**: (see Reader Properties on page 66 for more details about trustee functions)
  - **Intruder operator**: when the intruder alarm is set (see input properties), the reader used in conjunction with the intruder set up will only give access allowed to card holders whose type is set to "Intruder operator" or "Multi-card + Intruder"
  - **Extended Lock Release**: This option will allow the card holder to use the extended lock time set for the door.
- **Info Field 1 & 2**
  30 characters, no need to be unique. These fields provide a convenient way of recording information about the card holder - for example: vehicle registration number, telephone extension, etc. This information is visible in the Card Holder list in the Main Display when in Details view. The label of an information field can be edited by double-clicking it - note that this is a system-wide label that appears in every card-holder's properties.

Additional Information

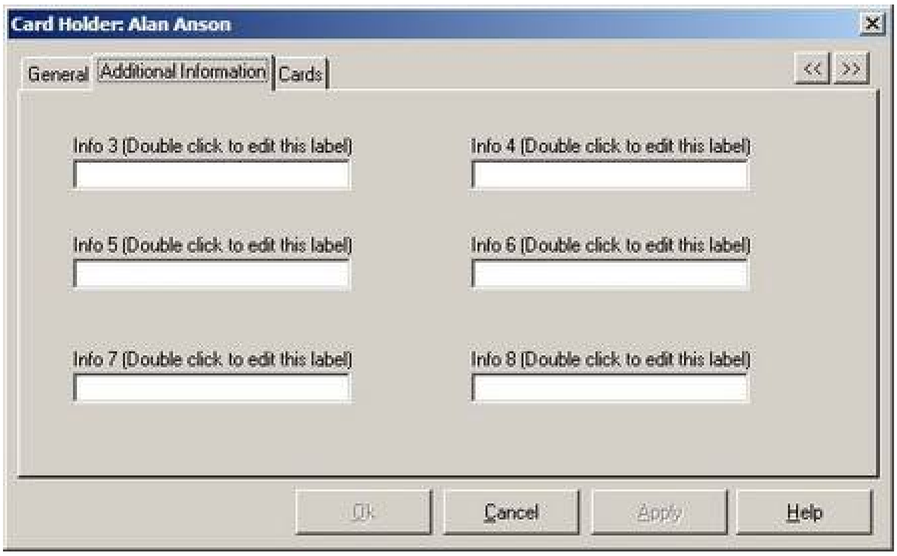
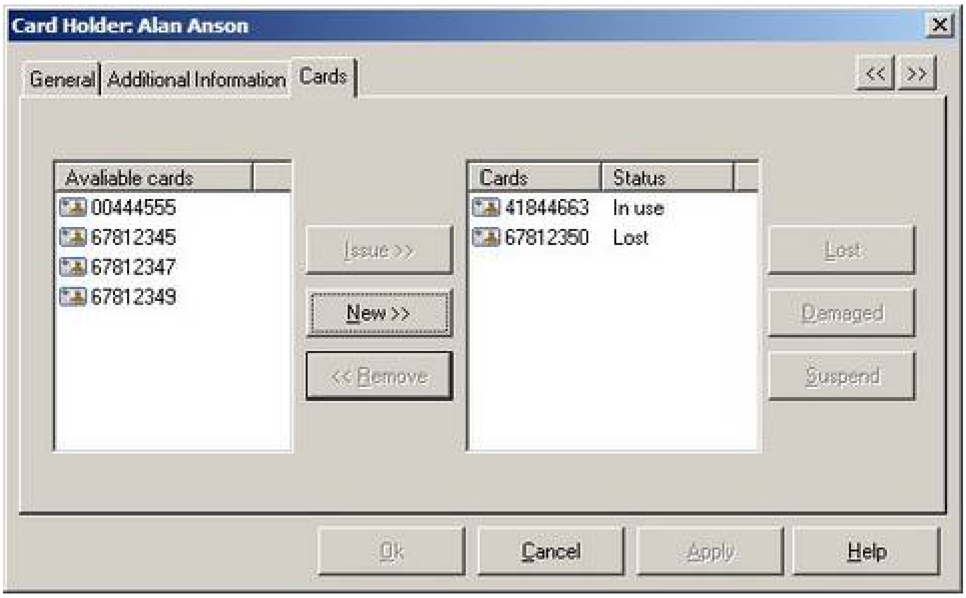

Card Holder: Alan Anson
General
Additional Information
Cards
<<
>>
Info 3 (Double click to edit this label)
Info 4 (Double click to edit this label)
Info 5 (Double click to edit this label)
Info 6 (Double click to edit this label)
Info 7 (Double click to edit this label)
Info 8 (Double click to edit this label)
Ok
Cancel
Apply
Help

Figure 40 Card Holder properties: Additional Information page

- **Info Fields 3-8**
  30 characters, no need to be unique. These fields provide a convenient way of recording information about the card holder - for example: vehicle registration number, telephone extension, etc. This information can be used for filtering and sorting operations when creating reports. The label of an information field can be edited by double-clicking it - note that this is a system-wide label that appears in every card-holder's properties.

Cards



Avaliable cards
00444555
67812345
67812347
67812349

Cards	Status
41844663	In use
67812350	Lost

Figure 41 Card Holder properties: Cards page

- **Available cards**
  Lists all cards that are already in the database and that are not issued to any card holder i.e. available. Select a card and click the **Issue** button for this to become associated with the card holder.

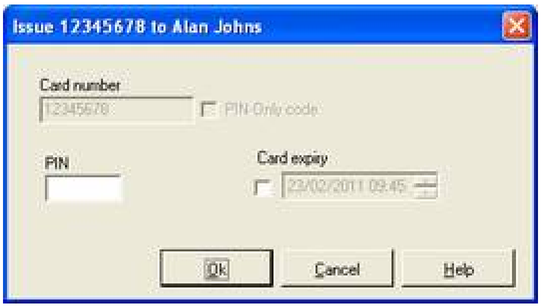
- **New**
  Click on this button to add a new card into the database and issue it to this card holder.
- **Issued cards**
  This is a list of all cards that are already issued to this card holder. Note that a card in this list may have been set as lost, damaged or suspended. Click on a card and click on one of the following to change the status of the card:
- **Remove**
  Makes the card available, so that it can later be re-issued to another Card-Holder. The card will not unlock doors until it is re-issued.
- **Lost, Damaged, Suspended**
  Stops the card from unlocking doors, but leaves it issued to the Card Holder.

Issuing cards

To assign a card to a user either:

- Select an available card on the Cards tab of the Card Holder properties and click on the issue button, or
- Click on the **New** button to add a new card to the database and assign it to the card holder.

If "*Prompt for card properties*" is enabled in System Settings (see page 33), the following dialog box is displayed:



Issue 12345678 to Alan Johns

Card number: 12345678

□ PIN-Only code

PIN:

Card expiry: □ 23/02/2011 09:45

Figure 42 Issuing a card

PIN
Enter a 4-digit PIN that will be associated with this card. If Card+PIN is turned on for a Reader, and that reader has a keypad fitted, then the card holder will be required to enter the PIN after using the card in order to unlock the door. If no PIN has been defined here, the card holder will be able to enter any PIN the first time the card is used for a Card+PIN entry, and that will become the allocated PIN for that card at that reader from then on. However, you will not be able to see what the PIN is in this window, and there will be a risk that a Card could end up with different PINs at different readers.

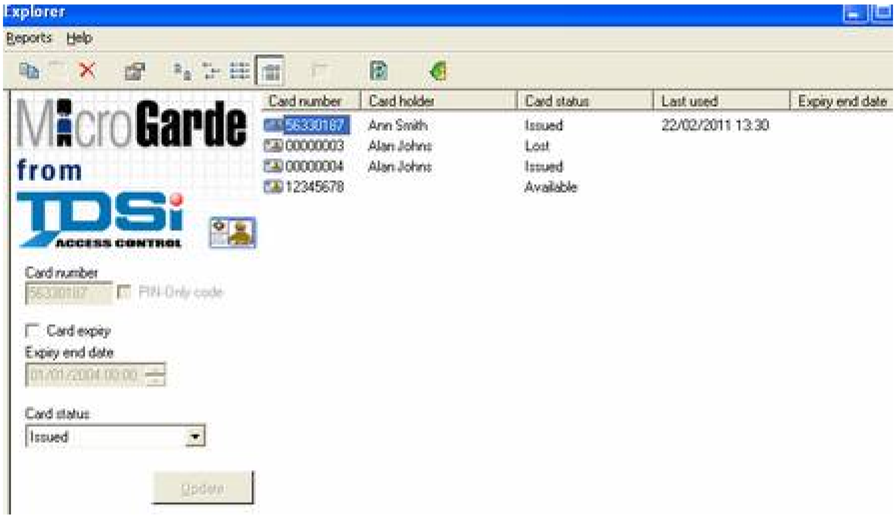
Card Expiry
If this box is checked then the card will automatically stop unlocking doors at the date and time specified.

5.2 Cards

Note that the term "Card" may refer to cards or key-fobs. Also, if your system has one or more Keypads fitted, the term "card" may also be used to refer to a Keypad code - i.e. a number that is typed at a keypad without a card needing to be used at all. MICROgarde software, and each MICROgarde controller, has capacity for 5000 cards.

5.2.1 Viewing Cards

To view existing cards, click on **Cards** in MICROgarde Explorer’s shortcut bar. MICROgarde Explorer lists the defined cards in the main display area.



Card number	Card holder	Card status	Last used	Expiry end date
56330187	Ann Smith	Issued	22/02/2011 13:30	
00000003	Alan Johns	Lost		
00000004	Alan Johns	Issued		
12345678		Available		

Card number: 56330187 ☐ PIN-Only code

☐ Card expiry

Expiry end date: 01/01/2004 00:00

Card status: Issued

Figure 43 Listing cards

Select a card to change some of its properties in the Quick Edit area:

- **Card Number**
  Eight digit code for card. You cannot change the number of a card in the database - this was fixed at the time it was entered.
- **PIN Code**
  If selected, the Card number field does not refer to a physical card - instead it refers to a number that can be typed at a keypad in order to unlock a door. You cannot change this property - this is fixed at the time it was entered.
- **Card Expiry**
  Select this check box to automatically stop the card unlocking doors at the date and time specified.
- **Card Status:**
  - *Issued*: the card has been allocated to a card holder.
  - *Available:* the card is not allocated to a card holder.
  - *Temporary issue*: the card will work exactly the same as an allocated card, but will automatically become "expired" after the number of days and hours specified in the System Settings.
  - *Lost, Damaged, Suspended*: the card is allocated to a card holder, but will not unlock any doors. The purpose of these options is to allow you to manage situations where some further action may be required. For

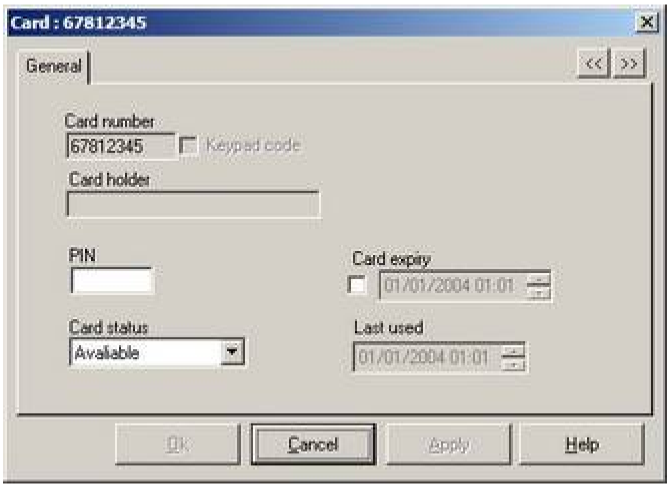
example, a lost card may become found and you will be able to see to whom it should be returned. Or, you may want to replace damaged cards on a weekly basis, rather than immediately when reported.

To view the detailed properties of a card, double-click on its number or right-click on it and select **Properties** from the context menu.

The *General* page of the card's properties is then displayed (see below).

5.2.2 Card Properties

General


Card : 67812345

Card number: 67812345

□ Keypad code

Card holder:

PIN:

Card expiry: □ 01/01/2004 01:01

Card status: Available

Last used: 01/01/2004 01:01

Figure 44 Card properties: General page

- **Card Number**
  This will always appear as eight digits, regardless of the true length of the card number as printed on the card. Shorter numbers will have leading zeros added to make it up to 8 digits. You cannot change the number of a card in the database - this was fixed at the time it was entered.
- **PIN Code**
  If this box is checked then the Card number field does not refer to a physical card - instead it refers to a number that can be typed at a keypad in order to unlock a door. You cannot change this property - this is fixed at the time it was entered. The default is a 4 digit pin code but this can be changed in the system settings to up to 8 digits.
- **Card Holder**
  If the card is currently allocated to a Card Holder, the name of the person appears here.
- **PIN**
  This allows you to enter a 4-digit PIN that will be associated with this card. If Card+PIN is turned on for a Reader, and that reader has a keypad fitted, then the card holder will be required to enter the PIN after using the card in order to unlock the door. If no PIN has been defined here, the card holder will be able to enter any PIN the first time the card is used for a Card+PIN entry, and that will become the allocated PIN for that card at that reader from then on. However, you will not be able to see what the PIN is in this window, and there will be a risk that a Card could end up with different PINs at different readers.
- **Card Status**
  This will normally show either "*issued*" or "*available*" (i.e. allocated to a Card Holder or not) but there are other possible entries:

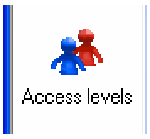
  - *Temporary issue*: the card will work exactly the same as an allocated card, but will automatically become "expired" after the number of days and hours specified in the System Settings.
  - *Lost, Damaged, Suspended*: the card is allocated to a card holder, but will not unlock any doors. The purpose of these options is to allow you to manage situations where some further action may be required. For example, a lost card may become found and you will be able to see to whom it should be returned. Or, you may want to replace damaged cards on a weekly basis, rather than immediately when reported.

- **Card Expiry**
  If this box is checked then the card will automatically stop unlocking doors at the date and time specified.
- **Last Used**
  This shows when the card was last used. This allows you to spot situations where a card holder has (say) two cards but is only using one on a regular basis. This may imply that the unused card has been lost but has not been reported.

5.3 Access Levels

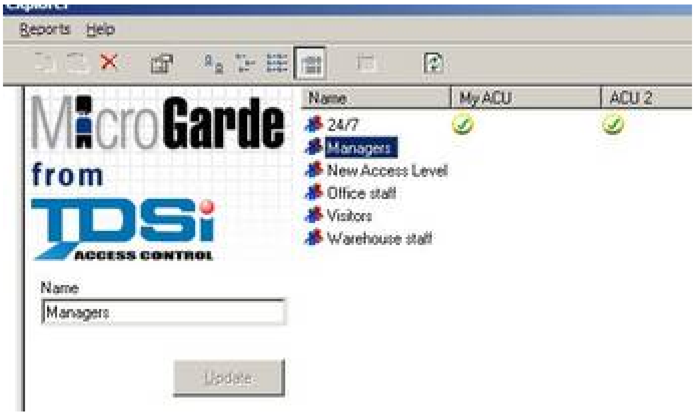
An Access Level provides a quick way of setting up who can go where. Instead of having to set up every card holder with a list of appropriate doors and time patterns, you simply allocate each card holder to an Access Level, which in turn is a list of appropriate readers and time patterns. Changing the properties of an Access Level automatically changes the access rights of every Card-Holder who is allocated to that level.

There is one pre-defined Access Level (‘*24-7*’) which automatically allows access through every Reader, all of the time. This cannot be modified or deleted.



To manage access levels, click on **Access Levels** in MICROgarde Explorer’s shortcut bar.

The main display area shows a list of all the Access Levels defined in the system. To change an Access Level’s name, select it and then edit as required in the Quick Edit area.



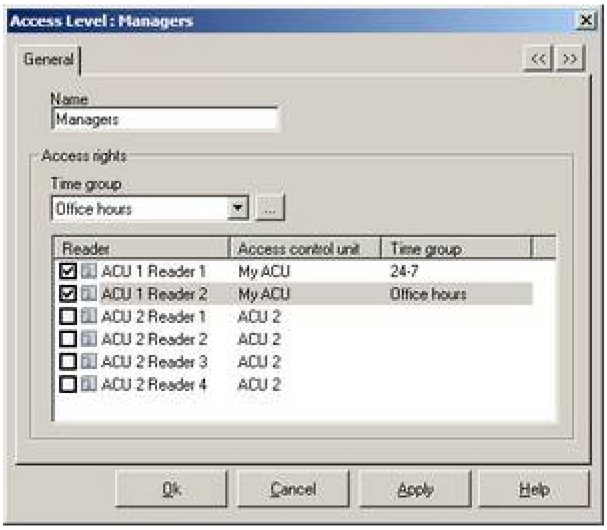
Name	My ACU	ACU 2
24/7	✓	✓
Managers		
New Access Level		
Office staff		
Visitors		
Warehouse staff		

Name: Managers

Figure 45 Listing Access Levels

- **Name**
  Name for this access level group: 30 characters, must be unique.
- **Time Group**
  Select a Time Group to allocate it to the currently-selected reader(s).

- **Reader & Time Pattern list**
  Select a Reader and Time Group to apply to the selected Access Group. The Access Group will be allowed access through this reader according to the rules in the time pattern listed to the right of the reader name.



Name: Managers

Access rights

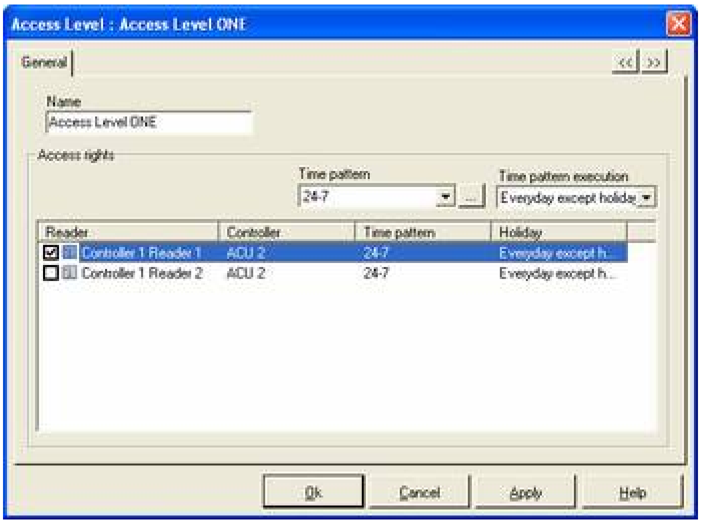
Time group: Office hours

Reader	Access control unit	Time group
☑ ACU 1 Reader 1	My ACU	24-7
☑ ACU 1 Reader 2	My ACU	Office hours
□ ACU 2 Reader 1	ACU 2	
□ ACU 2 Reader 2	ACU 2	
□ ACU 2 Reader 3	ACU 2	
□ ACU 2 Reader 4	ACU 2	

Figure 46 Access Level properties: General page

To change the associations and other properties of the access level, double-click on it. In its properties dialog box (see below), you can change the name, time pattern and time pattern execution.

Simply select the reader by clicking in the box next to the reader.



Name: Access Level ONE

Access rights

Time pattern: 24-7

Time pattern execution: Everyday except holiday

Reader	Controller	Time pattern	Holiday
☑ Controller 1 Reader 1	ACU 2	24-7	Everyday except h...
□ Controller 1 Reader 2	ACU 2	24-7	Everyday except h...

Figure 47 Access Level associations

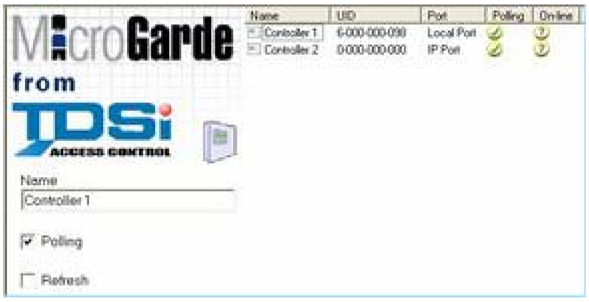
5.4 Controllers

A controller - sometimes abbreviated as an "Access Control Unit" or "ACU" - is the MICROgarde unit connected to the card readers, door locks, door sensors and exit buttons. The controller holds in memory the unique number of each Card that is to be allowed access through the Door(s), together with other appropriate information such as Time Patterns. In this way, the computer does not need to be running because the decision to open the door is taken entirely by the controller.

Some aspects of Controller configuration have already been described in the previous chapter (see page 36).

5.4.1 Viewing Controllers

To view existing controllers, click on **Controllers** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the installed controllers in the main display area.



Name	UID	Port	Polling	On-line
Controller 1	0-000-000-090	Local Port	✓	?
Controller 2	0-000-000-000	IP Port	✓	?

Name

Controller 1

☑ Polling

☐ Refresh

Figure 48 Listing Controllers

Select a controller to change the following properties in the quick edit area:

Name Change the name of the controller (30 characters max).

Polling Enable or disable polling of this controller for events.

Refresh Select Refresh and then click **Update** to rebuild the list of all cards and parameters. This may take some time (an event appears in the event list when the refresh has finished).

In the Details view, you can see additional information. Note that in this view, you can sort the list by clicking on a column title. In this view you can see whether the controllers are included in the polling list and also whether they are "on-line", i.e. communicating normally. A Question Mark in the On Line column indicates that there is a problem. Use the Troubleshooting section to resolve it.

The On-line column gives you further information about the controller:

Table 7 Controller Status icons

Icon	Status
✓	Off-line
?	On line

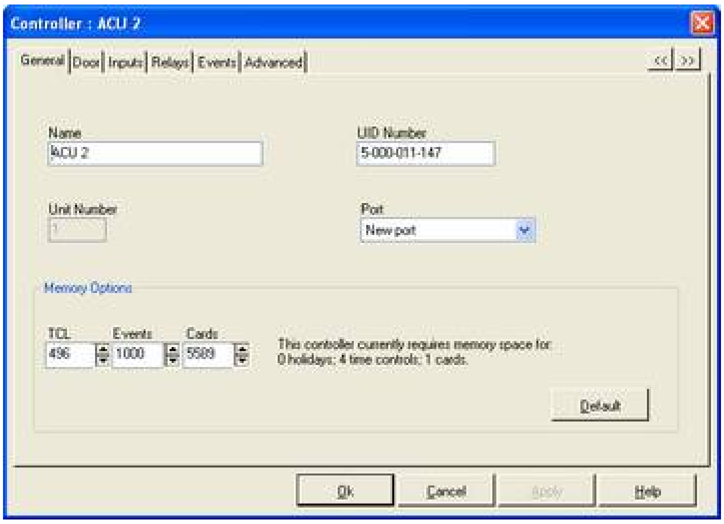
5.4.2 Controller Properties

To view the detailed configuration of a controller, double-click on the controller's name or right-click on it and select **Properties** from the context menu.

The *General* page of the controller's properties is then displayed (see below).

General

Use the *General* page to change the name of the controller, its Unit Number (if under software controller) and to set memory options.



Name: ACU 2

UID Number: 5-000-011-147

Unit Number: 1

Port: New port

TCL: 496

Events: 1000

Cards: 5589

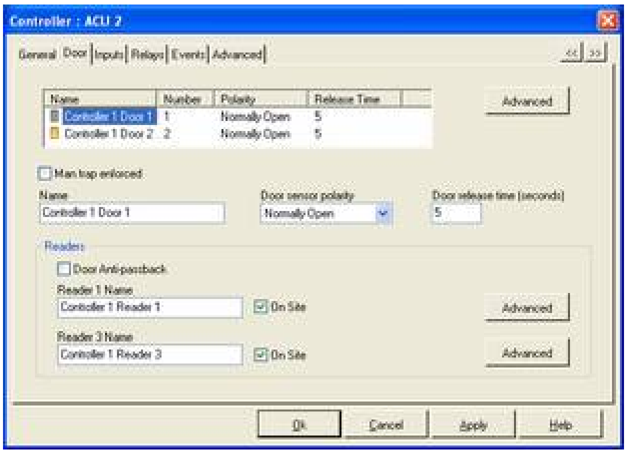
This controller currently requires memory space for: 0 holidays: 4 time controls: 1 cards.

Figure 49 Controller properties: General page

- **Name**
  30 characters, must be unique
- **UID Number**
  If the controller has been automatically detected, this number will have been automatically filled in for you but can be changed (in later versions of the software only). If you put the controller into the database without it having been detected, the number will be a string of zeroes. This number should be the same UID number written on the MICROgarde "chip".
- **Unit Number**
  This is the "address" of the controller, used for communications. The address of a controller is set by the rotary switch on its circuit board.
- **Memory Options**
  - **TCL** is a Time Control Line and generally 496 is plenty for the storage of programmed schedule lines, for example, *open a relay at 0730 on weekdays*.
  - **Events** are the number that will be stored in the MICROgarde should communications be stopped.
  - **Cards** are the maximum number of cards that the MICROgarde can store. These 3 partitions can be altered.

Door

Use each of the *Door* pages to set the names of the respective controlled door and its associated readers.



Name	Number	Polarity	Release Time
Controller 1 Door 1	1	Normally Open	5
Controller 1 Door 2	2	Normally Open	5

□ Man trap enforced

Name: Controller 1 Door 1

Door sensor polarity: Normally Open

Door release time (seconds): 5

□ Door Anti-passback

Reader 1 Name: Controller 1 Reader 1 ☑ On Site

Reader 3 Name: Controller 1 Reader 3 ☑ On Site

Figure 50 Controller properties: Door page

- **Name**
  30 characters, must be unique

- **Man trap enforced**
  This is only applicable for a controller that is controlling two doors. If this box is checked then the controller will not unlock one door if the other door is known to be open. This obviously requires that door sensors are fitted to both doors.

- **Door release time**
  The maximum length of time for which the door will be unlocked when a valid Card is used, or Exit button pressed, or a release command is sent from the MICROgarde PC software.

- **Door Sensor polarity**
  If a door sensor is fitted, then messages will be generated each time the door opens and closes (unless the messages are turned off). Depending upon the type of contacts fitted, you may need to change this setting. "*Normally open*" in this context means that the contacts are open when the door is open.

- **Door Anti-passback**
  This is only appropriate where two readers are fitted, one on either side of the door. Sometimes called "true anti-passback", this prevents a card being used twice in succession at the same Reader; i.e. after being used at an "in" Reader, a card must be seen at the "out" Reader before it can be used at the "in" Reader again.

  If you only have one Reader installed, then Timed Anti-passback may be used instead - you can set this up by clicking on **Advanced** next to the appropriate Reader, because it is set by the reader properties. Time anti –passback is to the reader only. See Reader Properties and Tab Options to set Timed anti-passback.

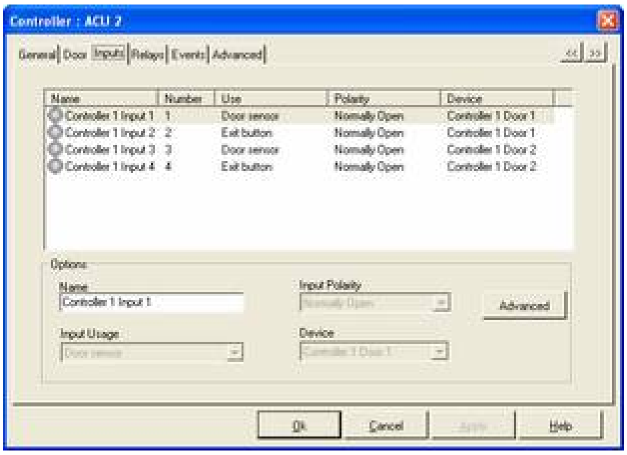
  True Anti-passback can be set with a Time Pattern by going into the Reader properties - you can set this up by clicking on **Advanced** next to the appropriate Reader. In Reader properties – Option tab, the Mode with be set to “Door” because you have selected True Antipassback option, but applying a Time Pattern for this Mode will set this time pattern up for the True Anti- Passback option selected.

- **Reader “x” Name**
  30 characters, must be unique. You can rename here or in the reader properties.
- **On Site**
  Check this box if you want a Card Holder to be recorded as being On-Site when they use this Reader. If you leave this unchecked then Card Holders will be recorded as Off-Site when they use this Reader.

  Click on the **Advanced** button to edit the Reader Properties (see page 66).

Inputs

The Inputs list shows all of the inputs on the controller. Click on an Input, and the configuration of that Input will be displayed in the *Options* group box.



Name	Number	Use	Polarity	Device
Controller 1 Input 1	1	Door sensor	Normally Open	Controller 1 Door 1
Controller 1 Input 2	2	Exit button	Normally Open	Controller 1 Door 1
Controller 1 Input 3	3	Door sensor	Normally Open	Controller 1 Door 2
Controller 1 Input 4	4	Exit button	Normally Open	Controller 1 Door 2

Options

Name: Controller 1 Input 1

Input Polarity: Normally Open

Advanced

Input Usage: Door sensor

Device: Controller 1 Door 1

Figure 51 Controller properties: Inputs page

Options for the selected input are:

- **Name**
  30 characters, must be unique
- **Input Polarity**
  This determines whether closed contacts across the Input results in an "on" message or an "off" message. Click on the **Advanced** button to view additional options for the Input. See Input Properties on page 70.
- **Input Usage**
  This selection determines what happens when the Input is turned on and off (note that in all cases the definition of "on" and "off" is determined by the Input Polarity setting, and the On and Off delays will also effect when the actions take place.) Depending on the number of Doors this controller is controlling, some or all of these Inputs may be reserved for use as Door Sense or Exit Button and you will not be able to change their usage.
  - *Unused*: only results in a message
  - *Door sense*: as well as a message, the use of a door sensor has the following effects:

    (a) When the door opens after a card, Exit button or software command, the lock relay is de-energized so that the door locks immediately on re-closure

    (b) If the door opens without a card, Exit button or software command, the *Door Forced* message is generated. This can be treated as an Abnormal event (Alarm icon will be next to event) (see *Events* on page 55) and can also trigger a Relay (See *Relays* on page 54)

(c) If the door opens for any reason, and stays on longer than the Local Alarm time, then the Local Alarm message is generated and a Relay may also be triggered.

(d) Similarly, if the door opens for any reason, and stays on longer than the Remote Alarm time, then the Remote Alarm message is generated and a Relay may also be triggered.

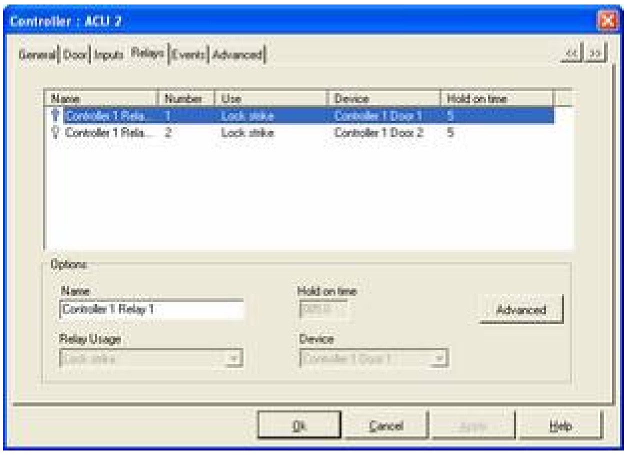
  - *Exit button*: the chosen door will be unlocked when the input is on. The lock relay is de-energized either when the door opens or when the lock strike time expires or when the Local Alarm is triggered.
  - *Control Relay*: the chosen relay will follow the input; i.e. the relay will be on when the input is on, and off when the input is off.
  - *Intruder Alarm Set*: when the input is on, access at the reader chosen in the Device field will only be allowed to card holders whose type is set to "Intruder operator" or "Multi-card + Intruder"
  - *Fire Activation*: when the input is on, all doors marked as Fire Doors are released.

- **Device**: This determines which object is affected by the input.

Relays

The Relays list shows all of the Relays on the controller. Click on a relay and the configuration of that relay will be displayed in the *Options* group box.

Note. To re-name a relay, close this window, click on the **Relays** shortcut, select the relay you want to re-name.



Controller : ACU 2

Name	Number	Use	Device	Hold on time
Controller 1 Rela...	1	Lock strike	Controller 1 Door 1	5
Controller 1 Rela...	2	Lock strike	Controller 1 Door 2	5

Options

Name: Controller 1 Relay 1

Hold on time: [illegible]

Relay Usage: Lock strike

Device: Controller 1 Door 1

Figure 52 Controller properties: Relays page

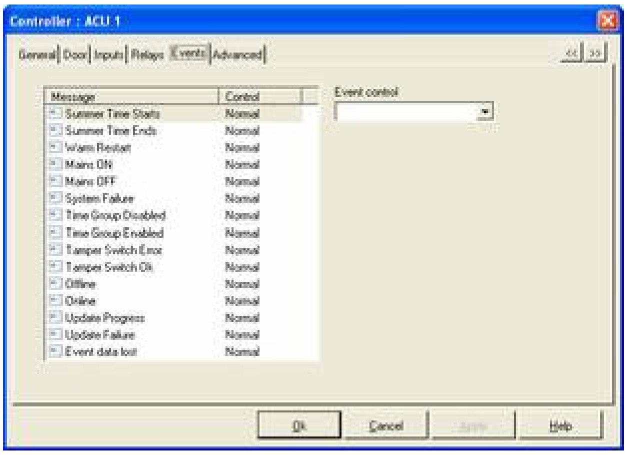
Options for the selected relay are:

- **Name**
  30 characters, must be unique
- **Hold On Time**
  For a Relay defined (in Relay Usage) as Lock Strike, this is the maximum length of time that a door is unlocked for when a valid card is used, or the Exit button is pressed and released, or a release command is issued from software. For any other relay, this is the additional length of time the relay remains on for after it would normally turn off.
- **Advanced**
  Brings up additional options for the Relay. See Relay properties on page 75.

- **Relay Usage**
  This determines what the relay is used for; i.e. the circumstances that will cause it to turn on and off:
  - *Unused*: the relay will only turn on when commanded to from the software.
  - *Lock Strike*: the relay will be used as the Lock Strike relay for the chosen door. Go to door properties for Lock Strike times.
  - *Door Shunt*: the relay will be used to shunt an intruder alarm; the relay turns on when the lock relay turns on, but turns off only when the door has closed. In that way, the Intruder system does not even know that the door has opened at all.
  - *Door Ajar pre Alarm and Door Ajar Alarm*: These features are described in the Door properties refer to that section in this manual.
  - *Door Forced*: the relay turns on if the door opens without a card, Exit button or software command. The relay stays on until the door closes.
  - *Duress Alarm*: the relay turns on if (a) Card+PIN is in use at the chosen reader and (b) someone uses a card and enters a PIN one digit higher in value (e.g. 1235 instead of 1234, or 6790 instead of 6789)
  - *Access Denied*: the relay turns on if access is denied for any reason (except too many wrong PINs)
  - *Too many wrong PINs*: the relay turns on if (a) Card+PIN is in use at the chosen reader and (b) someone uses a card and enters the wrong PIN four times in succession.
  - *Input*: the relay will follow the chosen input; i.e. the relay will be on when the input is on, and off when the input is off.
  - *Input Tamper*: if the input is configured as "supervised" instead of "digital", then the relay will turn on if a "tamper" condition is detected.
- **Device**
  This determines which object controls the relay - for example, if the Relay Usage is "*Door Forced*" then this is where you select the door.

Events

The Message list shows all of the event messages that can possibly be generated by the controller. If you click on an event, you can change the setting for that event in the Event Control field (see page 83).



Message	Control
Summer Time Starts	Normal
Summer Time Ends	Normal
Warm Restart	Normal
Mains ON	Normal
Mains OFF	Normal
System Failure	Normal
Time Group Disabled	Normal
Time Group Enabled	Normal
Tamper Switch Error	Normal
Tamper Switch Ok	Normal
Offline	Normal
Online	Normal
Update Progress	Normal
Update Failure	Normal
Event data lost	Normal

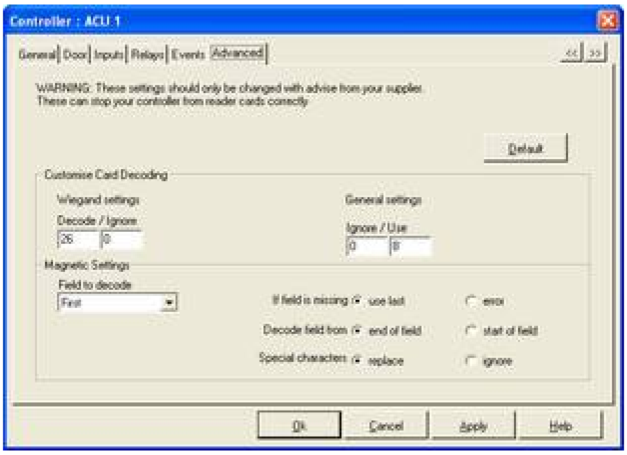
Event control

Figure 53 Controller properties: Events page

Advanced

The advanced properties of the controller should only be changed if you fully understand what you are changing as these will affect the way in the readers read the cards and therefore can stop the cards from being read.

> **Note.** These settings affect how the controller decodes data and have no effect on the reader itself. The options are for Wiegand or Magnetic (clock and data).



WARNING: These settings should only be changed with advise from your supplier.
These can stop your controller from reader cards correctly

Customise Card Decoding

Wiegand settings

Decode / Ignore: 26 / 0

General settings

Ignore / Use: 0 / 8

Magnetic Settings

Field to decode: First

If field is missing ● use last ○ error

Decode field from ● end of field ○ start of field

Special characters ● replace ○ ignore

Figure 54 Controller properties: Advanced page

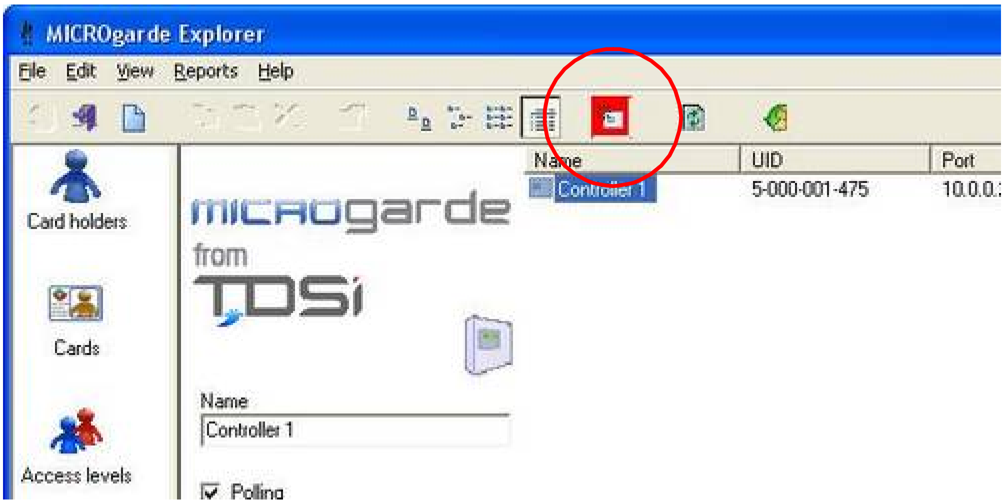
- **Default Button**
  If you make changes and find cards are no longer working, then this will set them back to the default settings.
- **Wiegand Settings**
  These are specific for a Wiegand interface.
  - **Decode**: Number of bits to decode
  - **Ignore**: Number of bits to ignore before decoding.
- **General Settings**
  These affect both Wiegand and Magnetic
  - **Ignore**: number of digits to ignore to determine the card number
  - **Use**: number of digits to determine the card number.
- **Magnetic Settings**: These are specific to a magnetic interface.
  - **Field to decode**: Magnetic cards may have numbers stored on the cards and separated by a field separator. This option allows you to determine which field to decode.
  - **If field is missing**: If you specify a particular field to decode and that field is not present, you either decode the previous field or do not decode any field and report an error.
  - **Decode field from**: A field may have more digits than what is required to determine the card number, this option allows you to specify either the start or end digits.
  - **Special Characters**: A field may be encoded with characters other than just digits. This allows you to either cover the character to a zero digit and use it as part of the number or ignore it and use the next character.

5.4.3 Adding a New Controller

Adding a New Controller using Autodetect

If a new controller is detected on the system (once the portal has been created), the “New ACU” icon on the top toolbar flashes (see page 36).

Note. You will need to add each ACU separately (either power up each ACU separately or plug them in to the RS485 line separately).



Name	UID	Port
Controller 1	5-000-001-475	10.0.0.:

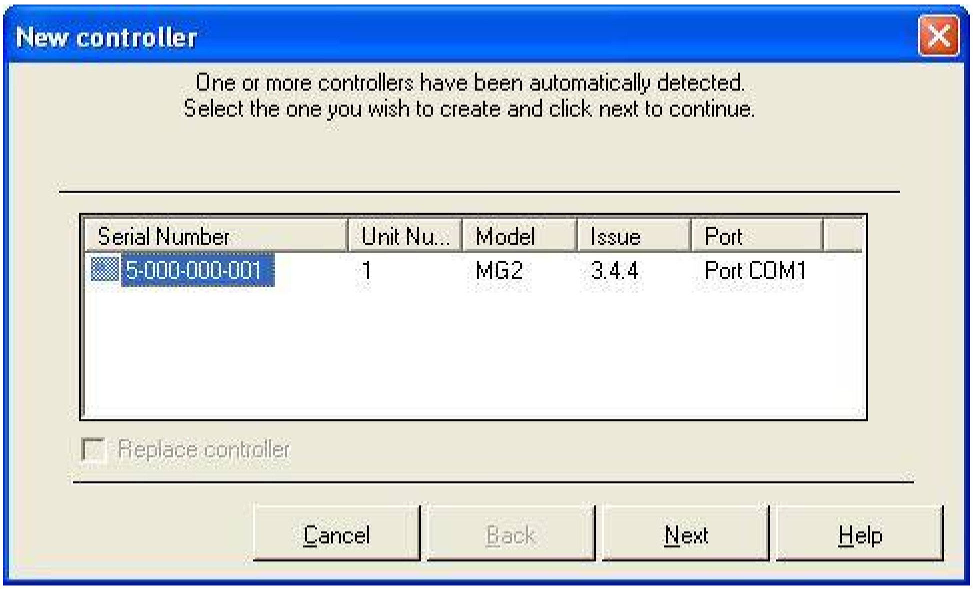
Name: Controller 1

☑ Polling

Figure 55 New ACU icon

To configure the detected ACU:

1. Click on the flashing **New ACU** button. The *New Controller* dialog box is displayed.



One or more controllers have been automatically detected.
Select the one you wish to create and click next to continue.

Serial Number	Unit Nu...	Model	Issue	Port
5-000-000-001	1	MG2	3.4.4	Port COM1

□ Replace controller

Figure 56 New Controller dialog box

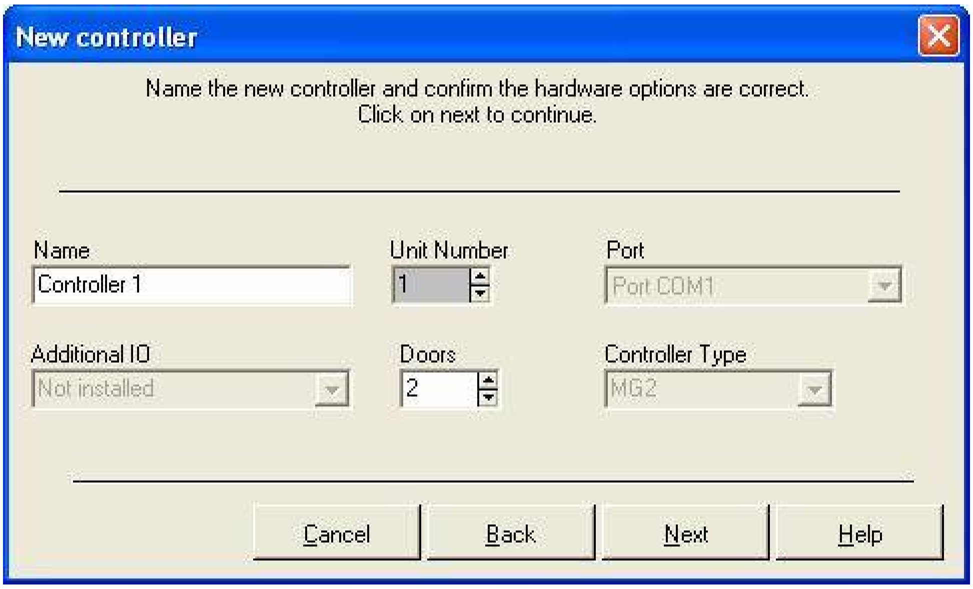
2. Click on the Serial Number (UID) of the ACU.

3. Click on the **Next** button.

4. Enter the following details:

   - **Name**
     Enter a name for the unit. This must be unique in the system and no more than 30 characters.
   - **Doors**
     Select the number of doors for that controller: 1 or 2.

   If auxiliary IO is being used, the *Additional IO* option will also be available.

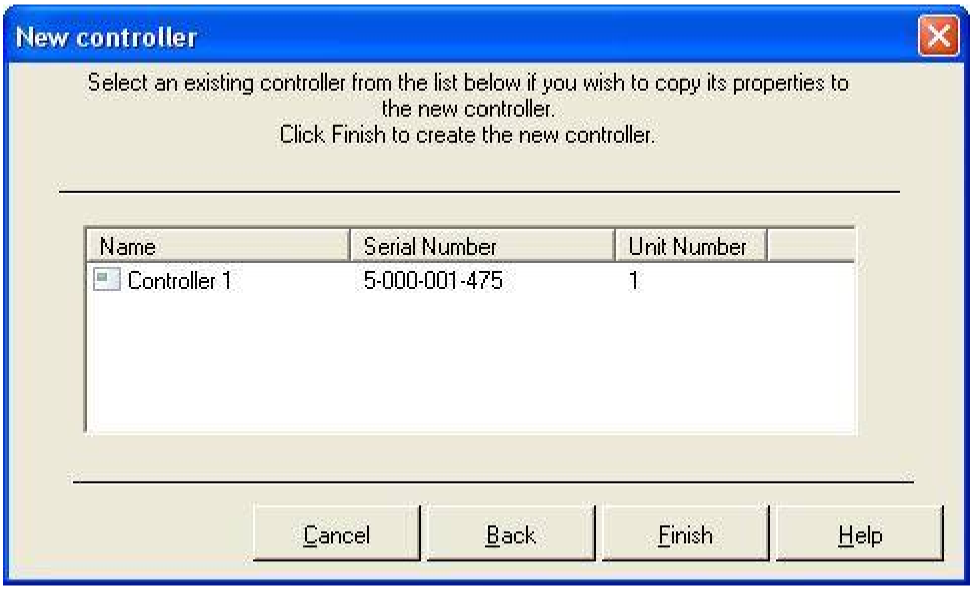

New controller

Name the new controller and confirm the hardware options are correct.
Click on next to continue.

Name: Controller 1
Unit Number: 1
Port: Port COM1
Additional IO: Not installed
Doors: 2
Controller Type: MG2

Figure 57 Naming the new controller

5. Click on **Next**. If you want to use an existing controller in the database as the basis for configuring the new one, select it from the displayed list. All settings will be copied except for object names (readers, doors etc.): these will be given default names.


New controller

Select an existing controller from the list below if you wish to copy its properties to the new controller.
Click Finish to create the new controller.

Name	Serial Number	Unit Number
Controller 1	5-000-001-475	1

Figure 58 Copying a configuration to the new controller

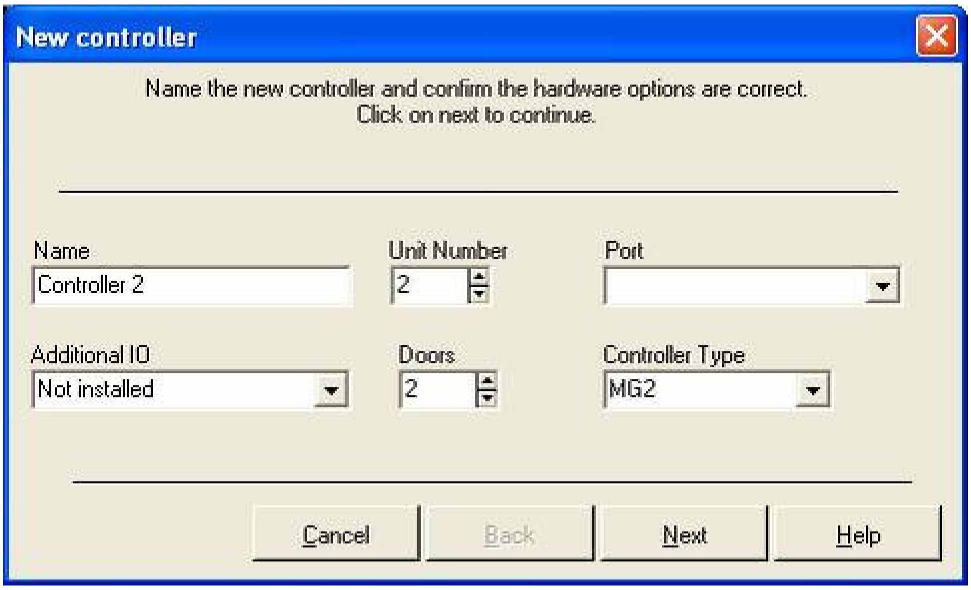
6. Click on the **Finish** button.

The new ACU is added to the MICROgarde software database and is online and ready for access control.

Adding a New Controller Manually

To add a new controller:

1. Click on the **New** button on the toolbar. The *New Controller* dialog box is displayed.



New controller

Name the new controller and confirm the hardware options are correct.
Click on next to continue.

Name: Controller 2

Unit Number: 2

Port:

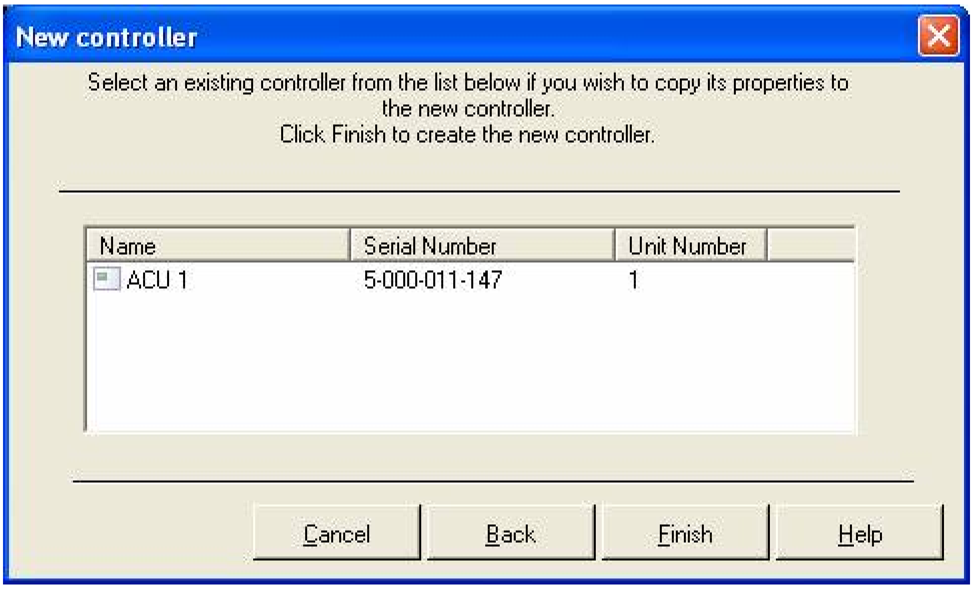
Additional IO: Not installed

Doors: 2

Controller Type: MG2

Figure 59 Adding a Controller

2. Enter the following details:
   - **Name**
     Enter a name for the unit. This must be unique in the system and no more than 30 characters.
   - **Unit Number**
     Dial or type the correct unit number for the controller
   - **Port**
     From the Port drop-down list box, select the port to which the controller is to be connected.
   - **Addition I/O**
     Specify whether the optional input/output module is connected.
   - **Doors**
     Select the number of doors for that controller: 1 or 2.
   - **Controller Type**
     Use the Controller Type drop-down list box to select the controller type: MG1 or MG2.
3. Click on the **Next** button. If you want to use an existing controller in the database as the basis for configuring the new one, select it from the displayed list. All settings will be copied except for object names (readers, doors etc.): these will be given default names.



New controller

Select an existing controller from the list below if you wish to copy its properties to the new controller.
Click Finish to create the new controller.

Name	Serial Number	Unit Number
ACU 1	5-000-011-147	1

Figure 60 Copying a Controller's properties

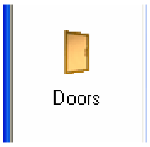
4. Click on **Finish** to complete the configuration.

5.5 Doors

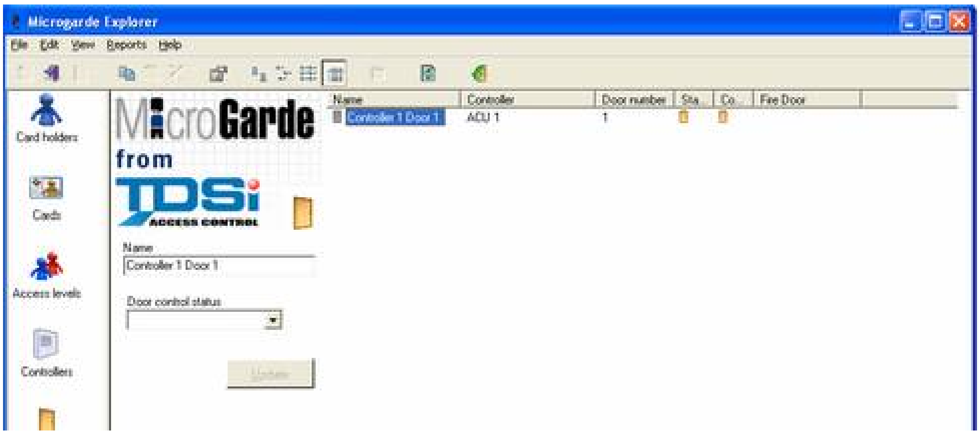
To provide access control, each door has up to three types of devices (excluding the reader or readers) associated with it:

- **Lock**: An electrically operated device with two possible states: locked or unlocked controlled by a relay on the Controller. On a MICROgarde unit, Relay 1 is the lock relay for door 1, and Relay 2 is the lock relay for door 2 (or is spare if the controller is only controlling one door).
- **Door sensor**: A switch that changes from open to closed, or closed to open, when the door opens. The state of the switch is detected by an input on the Controller. The use of a door sensor is optional.
- **Exit button**: This is usually a push-button fitted on the secure side of the door, that unlocks the door when pressed. Fitting an exit button is sometimes a cheaper option than fitting the type of lock than can be over-ridden by turning a handle or pushing a bar. If a door sensor is fitted, but no exit button or exit reader is fitted, then opening the door will result in a "door forced" message. The use of an Exit button is therefore optional where a door has one reader, and unnecessary when a door has two readers.

5.5.1 Viewing Doors



To view existing door configurations, click on **Doors** in MICROgarde Explorer’s shortcut bar. MICROgarde Explorer lists the defined doors in the main display area.



Name	Controller	Door number	Sta...	Co...	Fire Door
Controller 1 Door 1	ACU 1	1			

Name: Controller 1 Door 1

Door control status:

Figure 61 Listing Doors

Select a door to change its name or control status in the Quick Edit area.

- **Name**
  Change the name of the door (30 characters max)
- **Door control status**
  - *Lock door*: The door will remain locked (i.e. access will not be granted to valid cards, and the Exit button will not unlock the door) until one of the other three options is chosen
  - *Unlock door*: The door will remain unlocked until one of the other three options is chosen.
  - *Normal*: The door will operate normally

- *Release door*: The door will unlock for the pre-defined *Door Release Time* (set on the *General* page of *Door* properties, see below) and then return to *Normal* operation. This is true regardless of whether the door was previously controlled as Locked or Unlocked.

Status

The Status column provides further information about the door (if you have a door sensor fitted):

Table 8 Door Status icons

Icon	Status
?	Unknown
🚪✓	Open
✓	Closed
🚪	Forced
🚪i	Ajar Pre-alarm
🚪i	Ajar Alarm

Control Status

The Control Status column gives you further information about the door lock:

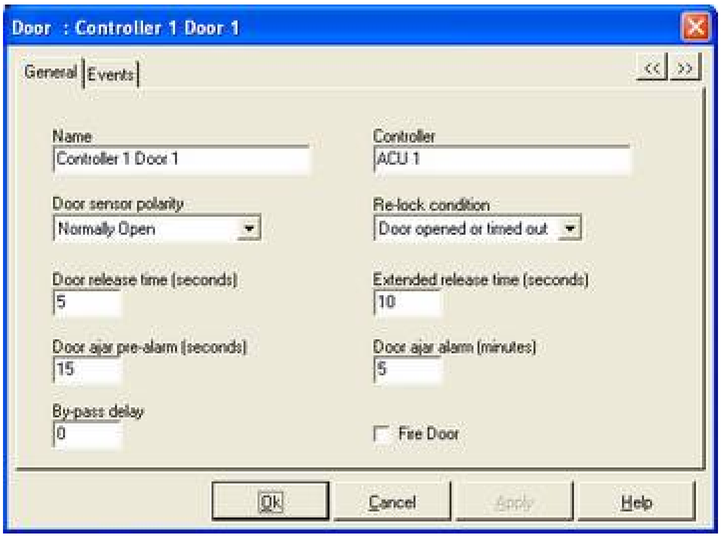
Table 9 Door Control Status icons

Icon	Status
?	Unknown
🔒	Locked
🔓	Unlocked
✓	Normal
🕒	Unlocked via Relay Time Pattern
🕒	Locked via Relay Time Pattern

5.5.2 Door Properties

To view the detailed configuration of a door, double-click on the door's name or right-click on it and select **Properties** from the context menu.

The *General* page of the door's properties is then displayed.



Name: Controller 1 Door 1

Controller: ACU 1

Door sensor polarity: Normally Open

Re-lock condition: Door opened or timed out

Door release time (seconds): 5

Extended release time (seconds): 10

Door ajar pre-alarm (seconds): 15

Door ajar alarm (minutes): 5

By-pass delay: 0

□ Fire Door

Figure 62 Door properties: General page

General

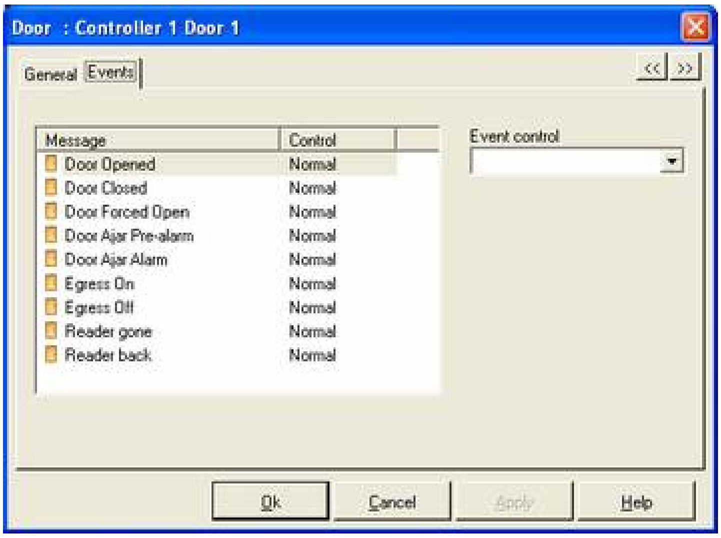
- **Name**
  30 characters, must be unique
- **Controller**
  This field shows which controller controls this door
- **Sensor Polarity**
  If a door sensor is fitted, then messages will be generated each time the door opens and closes (unless the messages are turned off). Depending upon the type of contacts fitted, you may need to change this setting. "Normally open" in this context means that the contacts are open when the door is open.
- **Re-Lock Condition**
  Allows the door to be relocked either when the door is opened, closed or after a preset time.
- **Door release time**
  This is the maximum length of time for which the door will be unlocked when a valid card is used, or the egress button is pressed, or a release command is sent from the MICROgarde PC software.
- **Extended Release Time**
  The extended lock time is used for employees that may require an extended time to proceed through the door and ensures that the system complies with the DDA (Disabilities Discrimination Act).
- **Door Ajar Pre-Alarm**
  If the door stays open for more than this time, then a "pre-alarm" event will be put into the event list. In addition, a relay may be triggered if one is configured to do so. The normal use of this feature is to use the relay to control a sounder near the door, to alert someone to the fact that it is still open.
- **Door Ajar Alarm**
  If the door stays open for more than this time, then an "alarm" event will be put

into the event list. In addition, a relay may be operated if one is configured to do so.

- **By-Pass Delay**
  Used to bypass the intruder entry circuit when integrating MICROgarde with Intruder Systems.
- **Fire Door**
  Check this box if the door is a Fire Door. All doors marked as Fire Doors are released when an input assigned as a Fire Activation input is activated.

Events

The Events tab displays a list of all the event messages that can be generated by the door. If you click on an event, you can change the setting for that event (see page 83).



Message	Control
Door Opened	Normal
Door Closed	Normal
Door Forced Open	Normal
Door Ajar Pre-alarm	Normal
Door Ajar Alarm	Normal
Egress On	Normal
Egress Off	Normal
Reader gone	Normal
Reader back	Normal

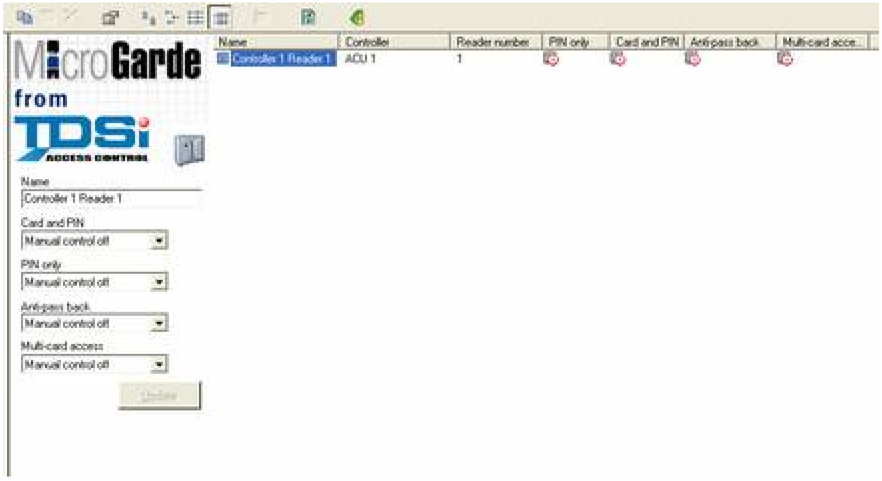
Figure 63 Door properties: Eventsl page

5.6 Readers

A "Reader" is any device that identifies the person attempting to gain access. Usually this will be a card reader, but sometimes it may be a simple keypad or it may be a biometric device that automatically recognizes some physical attribute of a person (fingerprint, iris pattern, etc.) and reports this to the controller as a unique number representing the person.

5.6.1 Viewing Readers

To view existing readers, click on **Readers** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the defined readers in the main display area.



Name	Controller	Reader number	PIN only	Card and PIN	Anti-pass back	Multi-card acce...
Controller 1 Reader 1	ACU 1	1	●	●	●	●

Name: Controller 1 Reader 1

Card and PIN: Manual control off

PIN only: Manual control off

Anti-pass back: Manual control off

Multi-card access: Manual control off

Figure 64 Listing Readers

Select a reader to change some of its basic properties in the Quick Edit area:

- **Name**
  Change the name of the reader (30 characters max)
- **Card and Pin, PIN only, Anti-pass back, Multicard access**

  Manual Control On: The mode is turned on, and will only turn off if another option is selected in this screen.

  Manual Control Off: The mode is turned off, and will only turn on if another option is selected in this screen.

  Timed Control: The mode will turn on and off according to any Time Pattern that has been defined in the Reader Properties screen.

  On, then Timed: The mode is turned on, and will then turn off and on according to any Time Pattern that has been defined in the Reader Properties screen. **Only available when you have assigned a time pattern.**

  Off, then Timed: The mode is turned off, and will then turn on and off according to any Time Pattern that has been defined in the Reader Properties screen. **Only available when you have assigned a time pattern.**

Status

The Status fields shows the setting chosen for each access mode:

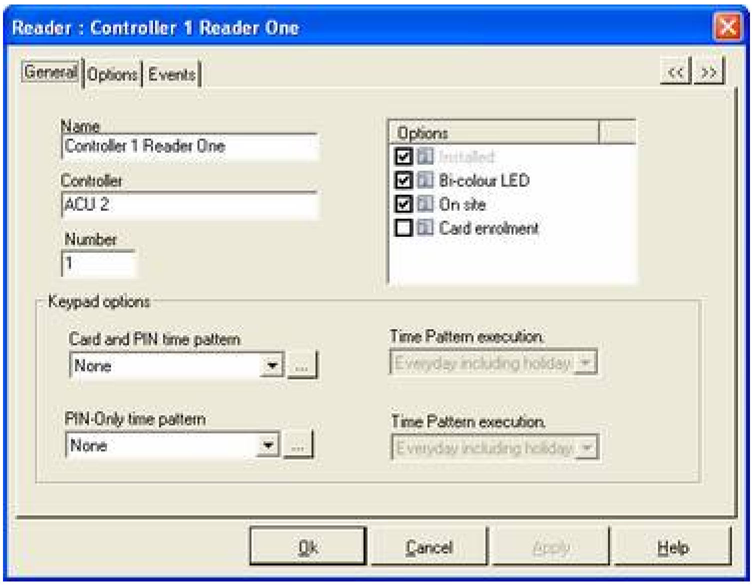
Table 10 Reader Status icons

Icon	Status
?	Unknown
✓	On
✕	Off
🕒	On, then Timed
🕒	Off, then Timed

5.6.2 Reader Properties

To view the detailed configuration of a reader, double-click on the reader's name or right-click on it and select **Properties** from the context menu.

The *General* page of the reader's properties is then displayed (see below).



Reader : Controller 1 Reader One

Name: Controller 1 Reader One

Controller: ACU 2

Number: 1

Options

☑ Installed

☑ Bi-colour LED

☑ On site

☐ Card enrolment

Keypad options

Card and PIN time pattern: None

Time Pattern execution: Everyday including holiday

PIN-Only time pattern: None

Time Pattern execution: Everyday including holiday

Figure 65 Reader properties: General page

General

- **Name**
  30 characters, must be unique
- **Controller**
  Controller connected to this reader.
- **Number**
  The Reader number.
- **Options**
- **Installed:** This indicates that this reader has been installed.
  - **On Site**: Check this box if you want a Card Holder to be recorded as being on-site when they use this reader. If you leave this unchecked then Card Holders will be recorded as off-site when they use this reader.
  - **Bi-color**: TDSi readers are fitted with two LEDs (green for access granted, red for access denied) and so this should be checked unless you are using non-TDSi readers. Even if other readers have 2 LED's

they are unlikely to be compatible - for further information please click here to see the Installation section

- **Card Enrolment**: Check this box if you want to use the reader as an enrolment reader.

- **Keypad Options**

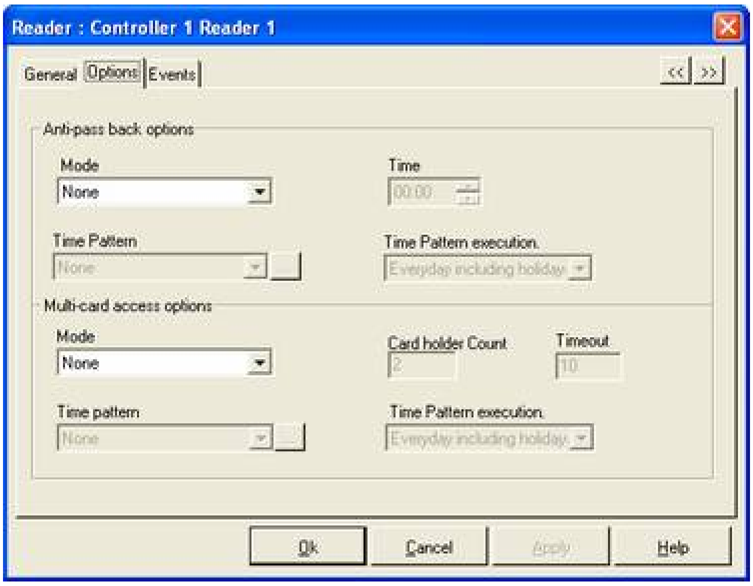
Select **Card and PIN** and/or **PIN-Only** time patterns. You can also define a new Time Pattern by clicking on the **Options** button:

If you want either of these modes to be permanently enabled, select *Manual Control On* as described previously.

Note. When **Card and PIN time pattern** is enabled, every card used will require a PIN to be entered before access is granted.

Options

Use this tab to set anti-passback and multicard options.



Anti-pass back options

Mode: None

Time: 00:00

Time Pattern: None

Time Pattern execution: Everyday including holiday

Multi-card access options

Mode: None

Card holder Count: 2

Timeout: 10

Time pattern: None

Time Pattern execution: Everyday including holiday

Figure 66 Reader properties: Options page

Anti-passback options

Choose whether Anti-passback options enabled (for this reader only) for a specific time pattern. You may choose to have Anti-passback turn on and off automatically by choosing a pre-defined time-pattern or you can define a new Time Pattern by clicking on the ... button.

Note. True Anti-passback is normally set for the Door rather than for individual readers. See Controller Properties (Door tab) on page 52.

If you want this mode to be permanently enabled, select *Manual Control On* as described previously.

Multi-card access options

Use these options to specify that more than one Card Holder may need to be present before access will be granted. At least one of these Card Holders must have been defined as a Trustee. When the Card Holder count is set to two, the possible modes of operation are:

- *Trustee plus*: requires two trustees

- *Trustee only*: requires only one trustee, but they must present their card twice
- *Trustee + card holder*: requires a Trustee plus any Normal Card Holder
- *Trustee + another*: requires a Trustee plus any other Card Holder (Trustee or Normal)

When the **Card holder Count** is set to more than 2 then, provided the conditions described above are met for two of the cards, the remaining cards can be either Normal or Trustee cards.

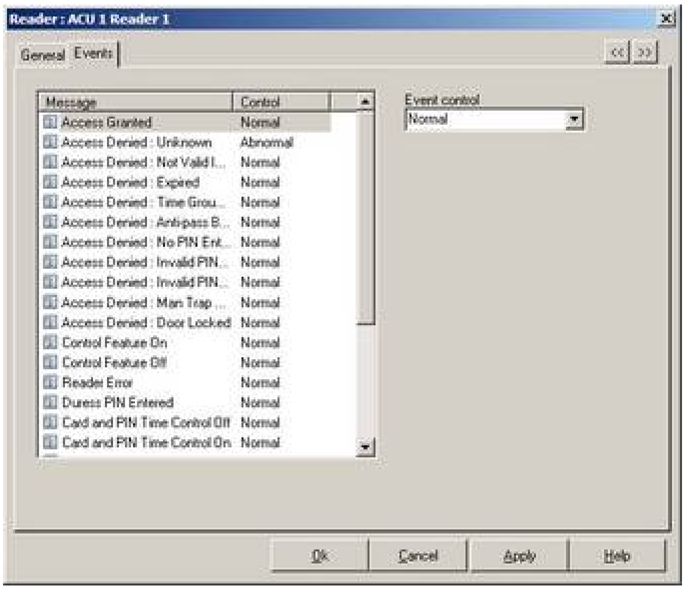
The **Timeout** period is the allotted time you have to present the access cards.

You may choose to have this feature turn on and off automatically by choosing a pre-defined time-pattern or you can define a new Time Pattern by clicking on the ... button:

If you want this mode to be permanently enabled, select *Manual Control On* as described previously.

Events

The Events tab displays a list of all the event messages that can be generated by the reader. If you click on an event, you can change the setting for that event (see page 83).



Reader : ACU 1 Reader 1

General | Events

Message	Control
Access Granted	Normal
Access Denied : Unknown	Abnormal
Access Denied : Not Valid I...	Normal
Access Denied : Expired	Normal
Access Denied : Time Grou...	Normal
Access Denied : Anti-pass B...	Normal
Access Denied : No PIN Ent...	Normal
Access Denied : Invalid PIN...	Normal
Access Denied : Invalid PIN...	Normal
Access Denied : Man Trap ...	Normal
Access Denied : Door Locked	Normal
Control Feature On	Normal
Control Feature Off	Normal
Reader Error	Normal
Duress PIN Entered	Normal
Card and PIN Time Control Off	Normal
Card and PIN Time Control On	Normal

Event control: Normal

Figure 67 Reader properties: Events page

5.7 Inputs

An input is a physical connection on the MICROgarde controller. By connecting a switch of some sort to an input (see Installation for details), the controller can respond appropriately (see below) and event messages can be seen in the MICROgarde Explorer.

Some inputs are reserved for special functions; inputs that are not reserved are referred to as "spare". An optional module is available that adds 4 spare inputs (as well as 2 spare relays). The following table shows the possible variations:

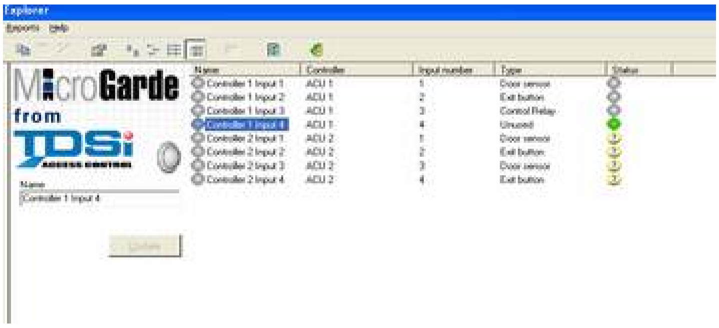
Table 11 Input configurations

Input Number	0-door configuration	1-door configuration	2-door configuration
1	spare	Door sensor	Door sense for Door 1
2	spare	Exit button	Exit button for Door 1
3	spare	spare	Door sense for Door 2
4	spare	spare	Exit button for Door 2
5 (if fitted)	spare	spare	spare
6 (if fitted)	spare	spare	spare
7 (if fitted)	spare	spare	spare
8 (if fitted)	spare	spare	spare

A spare input can be used to switch a relay. For more information on Door Sensor and Exit Button functionality, please refer to Doors.

5.7.1 Viewing Readers

To view existing inputs, click on **Inputs** in MICROgarde Explorer's shortcut bar. MICROgarde Explorer lists the defined inputs in the main display area.



Name	Controller	Input number	Type	Status
Controller 1 Input 1	ACU 1	1	Door sensor	○
Controller 1 Input 2	ACU 1	2	Exit button	○
Controller 1 Input 3	ACU 1	3	Control Relay	○
Controller 1 Input 4	ACU 1	4	Unused	●
Controller 2 Input 1	ACU 2	1	Door sensor	○
Controller 2 Input 2	ACU 2	2	Exit button	○
Controller 2 Input 3	ACU 2	3	Door sensor	○
Controller 2 Input 4	ACU 2	4	Exit button	○

Name: Controller 1 Input 4

Figure 68 Listing Inputs

Select an input to change its name in the Quick Edit area (30 characters max)

Status

The status column icons show the current state of each input.

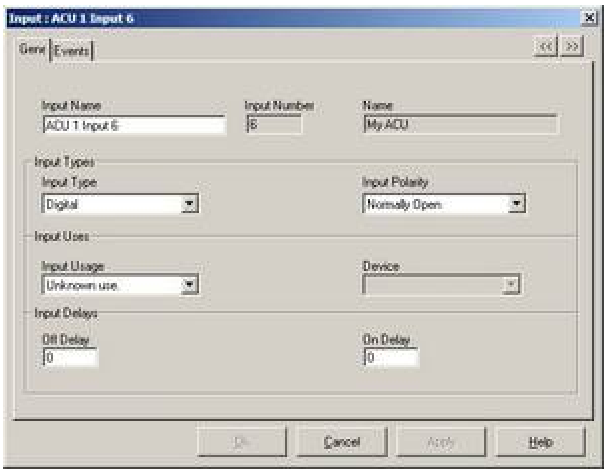
Table 12 Input Status icons

Icon	Status
?	Unknown
🟢	On
⚪	Off
🔴	Open circuit
🟢	Short-circuit

5.7.2 Input Properties

To view the detailed configuration of an input, double-click on the input’s name or right-click on it and select **Properties** from the context menu.

The *General* page of the input’s properties is then displayed (see below).



Input : ACU 1 Input 6

Input Name: ACU 1 Input 6
Input Number: 6
Name: My ACU

Input Types
Input Type: Digital
Input Polarity: Normally Open

Input Uses
Input Usage: Unknown use
Device:

Input Delays
Off Delay: 0
On Delay: 0

Figure 69 Input properties: General page

- **Input Name**
  30 characters, must be unique
- **Input number**
  The actual number of the input on the Controller.
- **Controller**
  Name of host controller.
- **Input Type**
  Determines whether the input is "digital" (i.e. it has two possible states - on and off) or "supervised" (i.e. it has three possible states - on, off and tamper). This in turn is determined by the installation – see page 18 for more details on supervised inputs.
- **Input Polarity**
  Determines whether closed contacts across the input results in an "on" message or an "off" message.
- **Input Usage**
  Determines what happens when the input is turned on and off (note that in all cases the definition of "on" and "off" is determined by the Input Polarity setting,

and the On and Off delays will also effect when the actions take place.) Depending on the number of doors this controller is controlling, some or all of these inputs may be reserved for use as Door Sense or Exit Button and you will not be able to change their usage.

- *Unused*: only results in a message
- *Door sense*: as well as a message, the use of a door sensor has the following effects:

  (a) When the door opens after a card, Exit button or software command, the lock relay is de-energized so that the door locks immediately on re-closure

  (b) If the door opens without a card, Exit button or software command, the Door Forced message is generated and a Relay may also be triggered.

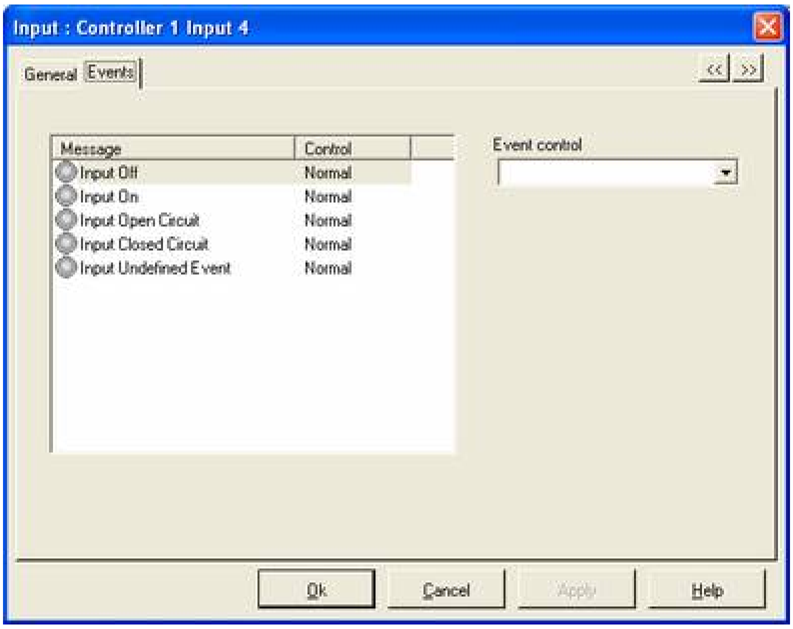
  (c) If the door opens for any reason, and stays on longer than the Local Alarm time, then the Local Alarm message is generated and a Relay may also be triggered.

  (d) Similarly, if the door opens for any reason, and stays on longer than the Remote Alarm time, then the Remote Alarm message is generated and a Relay may also be triggered.
- *Control Relay*: the chosen relay will follow the input; i.e. the relay will be on when the input is on, and off when the input is off.
- *Exit button*: the chosen door will be unlocked when the input is on. The lock relay is de-energized either when the door opens or when the lock strike time expires or when the Local Alarm is triggered.
- *Intruder Alarm Set*: when the input is on, access at the reader chosen in the Device field will only be allowed to card holders whose type is set to "Intruder operator" or "Multi-card + Intruder"

- **Device**
  Determines which object is affected by the input.
- **On Delay**
  If this figure is greater than 0, then the input will not be regarding as "on" until it has been in that state for the length of time specified. Note that if an input goes "off" again within this time period, it will not be regarded as having changed state at all.
- **Off Delay**
  If this figure is greater than 0, then the input will not be regarding as having gone "off" until it has been in that state for the length of time specified. Note that if an input goes "on" again within this time period, it will not be regarded as having changed state at all.

Events

The Events tab displays a list of all the event messages that can be generated by the input. If you click on an event, you can change the setting for that event (see page 83).



Message	Control
Input Off	Normal
Input On	Normal
Input Open Circuit	Normal
Input Closed Circuit	Normal
Input Undefined Event	Normal

Figure 70 Input properties: Events page

5.8 Relays

A relay is a part of the MICROgarde controller that allows you to control an external piece of equipment. For example, a relay is used to unlock a door by switching the power supply to the lock.

Some relays are reserved for special functions; relays that are not reserved are referred to as "spare". An optional module is available that adds 2 spare relays (as well as 4 spare inputs). The following table shows the possible variations:

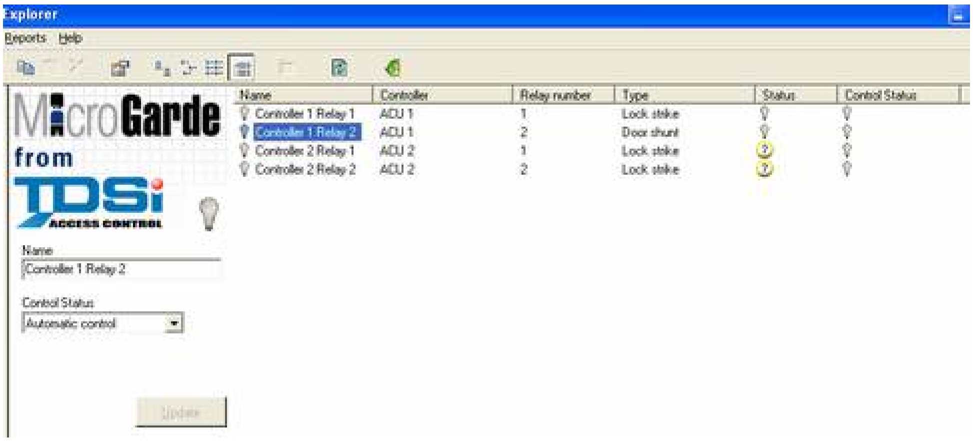
Table 13 Relay configurations

Relay Number	0-door configuration	1-door configuration	2-door configuration
1	spare	Lock Strike	Lock Strike for Door 1
2	spare	spare	
(but the default is Door shunt)	Lock Strike for Door 2		
3 (if fitted)	spare	spare	spare
4 (if fitted)	spare	spare	spare

A spare relay can be switched by an Alarm event, a Time Pattern or a manual command.

5.8.1 Viewing Relays

To view existing relays, click on **Relays** in MICROgarde Explorer’s shortcut bar. MICROgarde Explorer lists the defined relays in the main display area.



Name	Controller	Relay number	Type	Status	Control Status
Controller 1 Relay 1	ACU 1	1	Lock strike	💡	💡
Controller 1 Relay 2	ACU 1	2	Door shunt	💡	💡
Controller 2 Relay 1	ACU 2	1	Lock strike	?	💡
Controller 2 Relay 2	ACU 2	2	Lock strike	?	💡

Name: Controller 1 Relay 2

Control Status: Automatic control

Figure 71 Listing Relays

Select a relay to change some of its basic properties in the Quick Edit area:

- **Name**
  Change the name of the relay (30 characters max)
- **Control Status**

  Manual Control On: The relay is turned on, and will only turn off if another option is selected in this screen.

Manual Control Off: The relay is turned off, and will only turn on if another option is selected in this screen.

Automatic Control: The relay will turn on and off according to any Time Pattern that has been defined in the Reader Properties screen.

Timed Control On: The relay is turned on, and will then turn off and on according to any Time Pattern that has been defined in *Reader Properties* (see page 66). This option is only available if the relay has a time pattern associated with it.

Timed Control Off: The relay is turned off, and will then turn on and off according to any Time Pattern that has been defined in *Reader Properties* (see page 66). This option is only available if the relay has a time pattern associated with it.

Pulse: The relay turns on for the pre-defined hold-on time.

Status

In a Details view, the Status column shows you the state for each relay:

Table 14 Relay Status icons

Icon	Status
?	Unknown
✓	On
💡	Off

Control Status

In a Details view, the Control Status column shows you further information about any operator-defined settings for this relay:

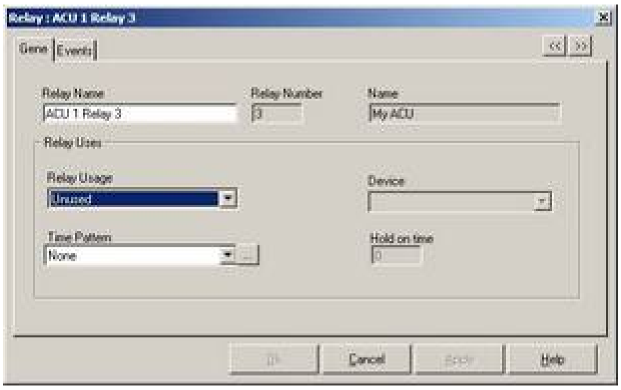
Table 15 Relay Control Status icons

Icon	Status
?	Unknown
✓	On
✗	Off
💡	Automatic
🕒	On then Automatic
🕒	Off then Automatic

5.8.2 Relay Properties

To view the detailed configuration of a relay, double-click on the relay's name or right-click on it and select **Properties** from the context menu.

The *General* page of the relay's properties is then displayed (see below).



Relay : ACU 1 Relay 3

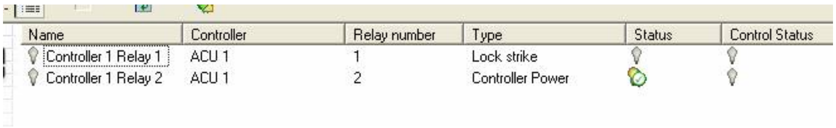
Relay Name: ACU 1 Relay 3
Relay Number: 3
Name: My ACU

Relay Uses
Relay Usage: Unused
Device:
Time Pattern: None
Hold on time: 0

Figure 72 Relay properties: General page

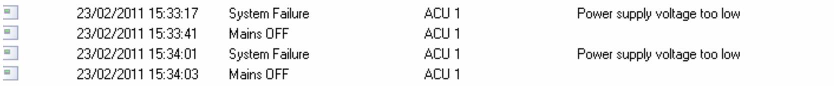
- **Relay Name**
  30 characters, must be unique
- **Relay number**
  The actual number of the Relay on the Controller.
- **Controller**
  Controller hosting this Relay.
- **Relay Usage**
  This determines what the relay is used for; i.e. the circumstances that will cause it to turn on and off:
  - *Unused*: the relay will only turn on when commanded to from the software.
  - *Lock Strike*: the relay will be used as the Lock Strike relay for the chosen door.
  - *Door Shunt*: the relay will be used to shunt an intruder alarm; the relay turns on when the lock relay turns on, but turns off only when the door has closed. In that way, the Intruder system does not even know that the door has opened at all.
  - *Door Ajar Pre-Alarm*:
  - *Door Ajar (Local) and Door Ajar (Remote)*: These features are described in the Door properties section: see page 63.
  - *Door Forced*: the relay turns on if the door opens without a card, Exit button or software command. The relay stays on until the door closes.
  - *Duress Alarm*: the relay turns on if (a) Card+PIN is in use at the chosen reader and (b) someone uses a card and enters a PIN one digit higher in value (e.g. 1235 instead of 1234, or 6790 instead of 6789)
  - *Access Denied*: the relay turns on if access is denied for any reason (except too many wrong PINs)
  - *Too many wrong PINs*: the relay turns on if (a) Card+PIN is in use at the chosen reader and (b) someone uses a card and enters the wrong PIN four times in succession.

- *Input*: the relay will follow the chosen input; i.e. the relay will be on when the input is on, and off when the input is off.
- *Input Fault*: if the input is configured as "supervised" instead of "digital", then the relay will turn on if a "tamper" condition is detected.
- *Intruder By-pass*: The relay (wired to the intruder panel) informs the intruder system whenever access is granted, so that the intruder system can enable the entry timer. If the front door opens for any reason other than this, because the entry timer remains disabled the alarm will be raised immediately.
- *Tamper Switch*: the relay turns on if the tamper is triggered (controller case opened)
- *Controller Power*: the relay triggers active (see status column of relay below) when the power of the ACU drops below the 12.7V threshold and reports power supply voltage too low in the events screen



Name	Controller	Relay number	Type	Status	Control Status
Controller 1 Relay 1	ACU 1	1	Lock strike		
Controller 1 Relay 2	ACU 1	2	Controller Power		

Events appear as below



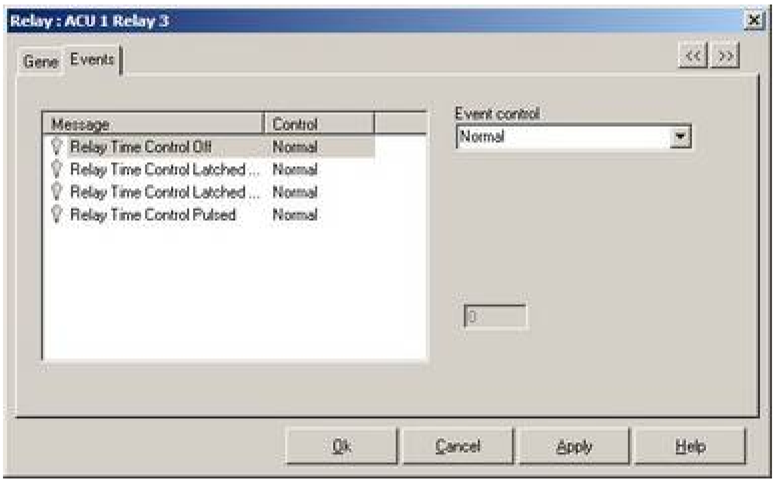
23/02/2011 15:33:17	System Failure	ACU 1	Power supply voltage too low
23/02/2011 15:33:41	Mains OFF	ACU 1	
23/02/2011 15:34:01	System Failure	ACU 1	Power supply voltage too low
23/02/2011 15:34:03	Mains OFF	ACU 1	

- **Device**
  This determines which object controls the relay - for example, if the Relay Usage is "Door Forced" then this is where you choose which Door.
- **Time Pattern**
  This allows you to have a Relay turn on and off automatically according to a pre-defined time-pattern, or you can define a new Time Pattern by clicking on the ... button.

If you want a relay to be permanently on, select *Manual Control On* as described previously.

Events

The Events tab displays a list of all the event messages that can be generated by the relay. If you click on an event, you can change the setting for that event (see page 83).



Relay : ACU 1 Relay 3

Message	Control
Relay Time Control Off	Normal
Relay Time Control Latched ...	Normal
Relay Time Control Latched ...	Normal
Relay Time Control Pulsed	Normal

Event control: Normal

0

Figure 73 Relay properties: Events page

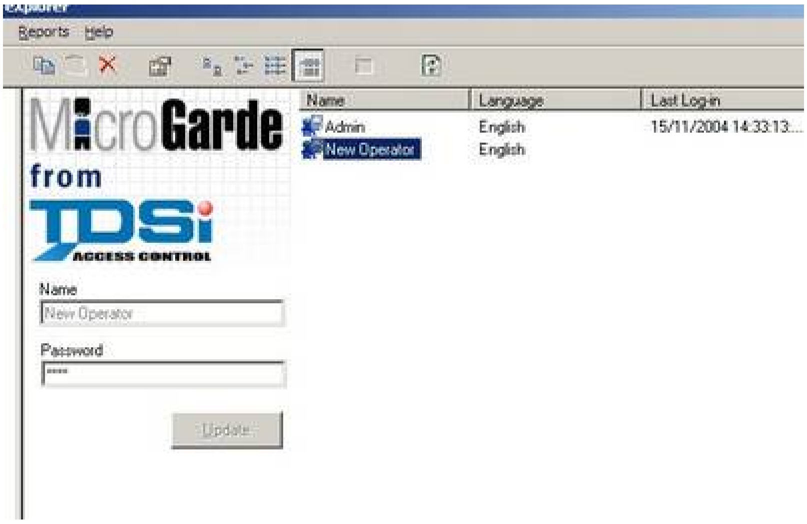
5.9 Operators

Operators are the users who have access to the MICROgarde software in order to make changes or view information. Different operators can have different rights to view and change information.

The Admin operator is already pre-defined, with a password of 1234 but upon first logging in you may have already changed this. This Admin operator cannot be deleted or renamed. But we suggest you change this password, and make a note of it somewhere safe and secure. If you lose this password, and no other operator has Full Rights to Operators, the system may become unusable because you may not be able to make another operator with full access rights.

5.9.1 Viewing Operators

To view existing operators, choose **View > Operators**. MICROgarde Explorer lists the defined operators in the main display area.



Name	Language	Last Log-in
Admin	English	15/11/2004 14:33:13...
New Operator	English	

Name: New Operator

Password: ****

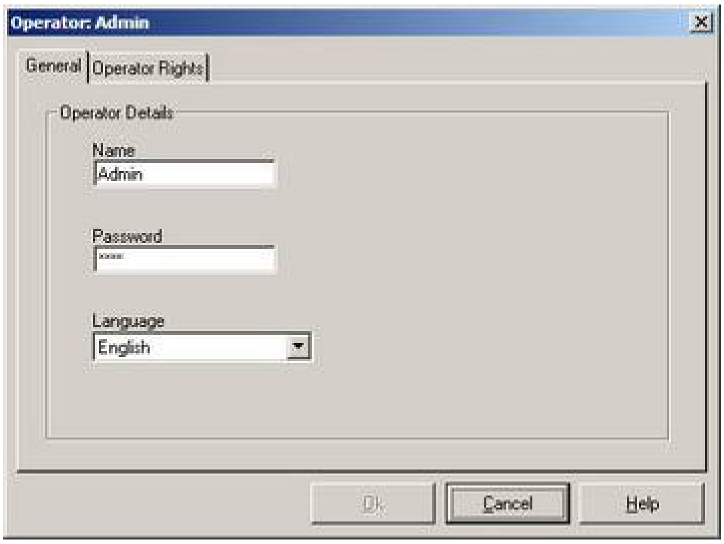
Figure 74 Listing Operators

Select an operator to change their password in the Quick Edit area:

- **Name**
  Up to 30 characters; must be unique in the entire list of operators. When the operator enters their name at the time of logging on, they must use the same case.
- **Password**
  Up to 10 characters (numbers and letters only)

To view the detailed properties of an operator, double-click on their name or right-click on it and select **Properties** from the context menu.

The *General* page of the operator's properties is then displayed (see below).



Operator Details

Name: Admin

Password: ****

Language: English

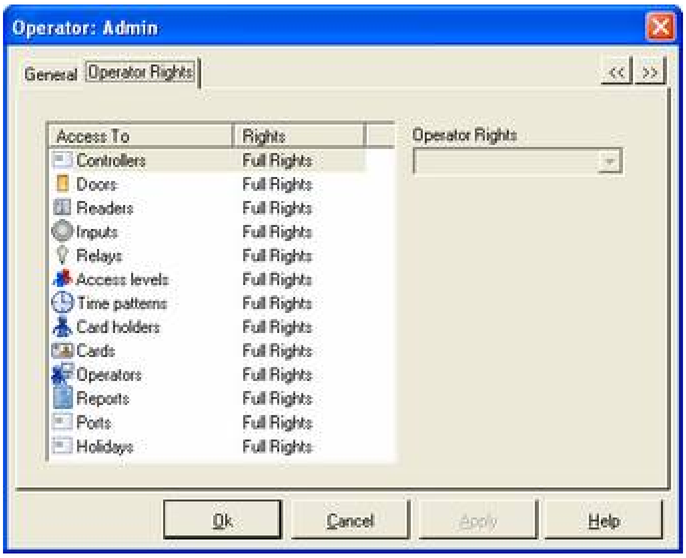
Figure 75 Operator properties: General page

The General page allows you to change the following operator details:

- **Name**
  Up to 30 characters; must be unique in the entire list of operators. When the operator enters their name at the time of logging on, they must use the same case.
- **Password**
  Up to 10 characters (numbers and letters only)
- **Language**
  The language which MICROgarde will use for displays, messages and reports when this operator is logged in.

Operator Rights

The Operator Rights tab lists all of the object types in the system, and the rights that this operator will have to those objects when logged in.



Access To	Rights
Controllers	Full Rights
Doors	Full Rights
Readers	Full Rights
Inputs	Full Rights
Relays	Full Rights
Access levels	Full Rights
Time patterns	Full Rights
Card holders	Full Rights
Cards	Full Rights
Operators	Full Rights
Reports	Full Rights
Ports	Full Rights
Holidays	Full Rights

Figure 76 Operator properties: Operator Rights page

To change the rights, select an item in the list and then choose the appropriate access privilege:

- *Full Rights*: If an operator has Full Rights to Operators then he or she will be able to change all of their other rights when they are logged on. Therefore only the most trustworthy person should have Full Rights to Operators.
- *User Rights*: Allows a general user operator setting which allows limited control with editing allowed for cards and cardholders.
- *View Rights*: these rights allow only to see the icons and objects and NO editing/deleting/adding enabled.
- *No Rights*: Choosing "No Rights" for any particular object mean that the Operator won't even see that they exist. If you click on an object, you can change the setting for that object in the Access Rights field.

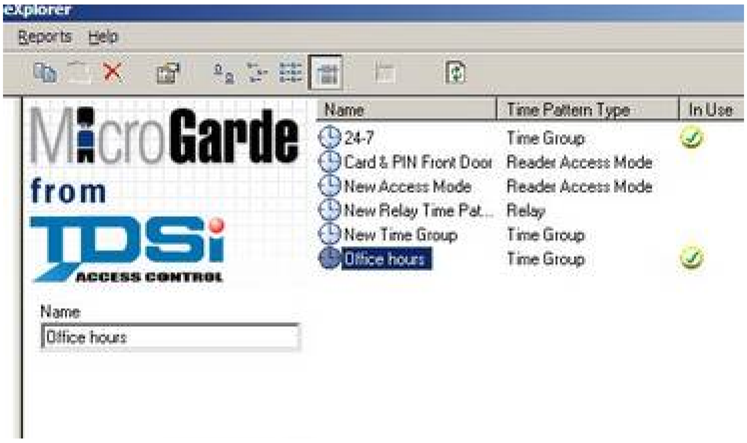
Repeat this procedure for all the access rights you want to change.

5.10 Time Patterns

Time patterns are used to control three type of object: *Relays*, *Access Levels* and *Reader Access Modes*. When you create a Time Pattern, you must specify what type of object it will be used to control. There is one Access Level Time Pattern pre-defined (24-7) in the system which automatically allows access through every Reader, all of the time. This cannot be modified or deleted.

5.10.1 Viewing Time Patterns

To view existing time patterns, choose **View > Time Patterns**. MICROgarde Explorer lists the defined time patterns in the main display area.



Name	Time Pattern Type	In Use
24-7	Time Group	✓
Card & PIN Front Door	Reader Access Mode	
New Access Mode	Reader Access Mode	
New Relay Time Pat...	Relay	
New Time Group	Time Group	
Office hours	Time Group	✓

Name: Office hours

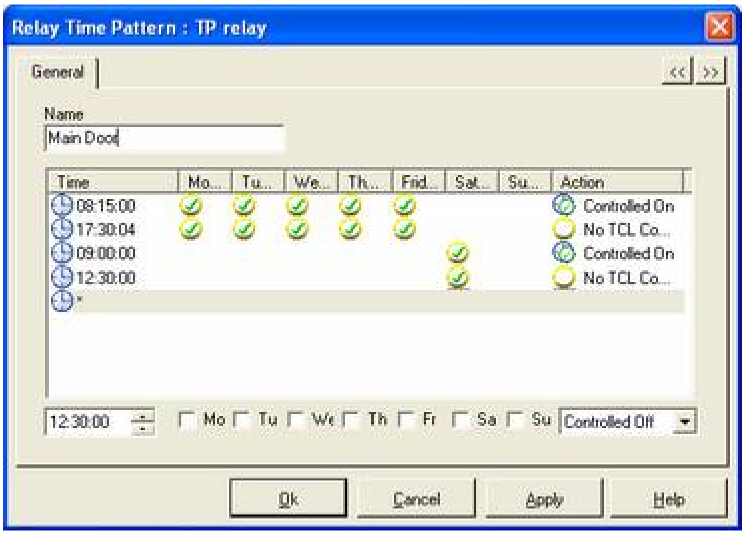
Figure 77 Listing Time Patterns

Select a time pattern to edit its name in the Quick Edit area:

- **Name**
  Up to 30 characters; must be unique in the entire list of time patterns.

To view the detailed properties of a time pattern, double-click on its name or right-click on it and select **Properties** from the context menu.

The *General* page of the Time Pattern’s properties is then displayed (see below).



Name: Main Door

Time	Mo...	Tu...	We...	Th...	Frid...	Sat...	Su...	Action
08:15:00	✓	✓	✓	✓	✓			Controlled On
17:30:04	✓	✓	✓	✓	✓			No TCL Co...
09:00:00						✓		Controlled On
12:30:00						✓		No TCL Co...
*								

12:30:00 □ Mo □ Tu □ We □ Th □ Fr □ Sa □ Su Controlled Off

Figure 78 Time Pattern properties: General page

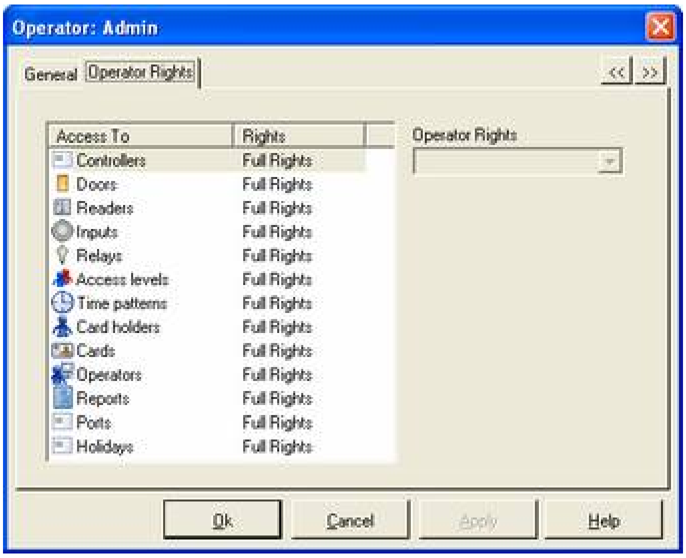
The General page allows you to build a list of times, days and actions that will affect any object which it is used to control.

To add a new line in the list:

1. Click on the last (empty) line in the list.
2. Select the time and days to define this time pattern.
3. Choose the time pattern's action. Possible actions for all object types are *Controlled ON* and *Controlled OFF*. Relays have two additional actions:
   - *No TCL control*: Allows the relay to operate according to its Properties settings; for example a Lock Strike relay could have a time pattern that causes the door to be unlocked (Controlled ON) from 9 A.M. each day; at 5 P.M. the Relay would be set to "No TCL Control" which means that the Relay will operate when a valid card is used. (Controlled OFF in this instance would lock the door permanently)
   - *Pulse*: If you want a relay to operate only briefly then only one line is needed, with the action type set to Pulse. The Relay will come on for the length of the Hold On time set in the Relay's Properties.
4. Click on the **OK** button to finish.

Operator Rights

The Operator Rights tab lists all of the object types in the system, and the rights that this operator will have to those objects when logged in.



Access To	Rights
Controllers	Full Rights
Doors	Full Rights
Readers	Full Rights
Inputs	Full Rights
Relays	Full Rights
Access levels	Full Rights
Time patterns	Full Rights
Card holders	Full Rights
Cards	Full Rights
Operators	Full Rights
Reports	Full Rights
Ports	Full Rights
Holidays	Full Rights

Figure 79 Time Pattern properties: Operator Rights

To change operator rights, choose the appropriate access privilege for each item:

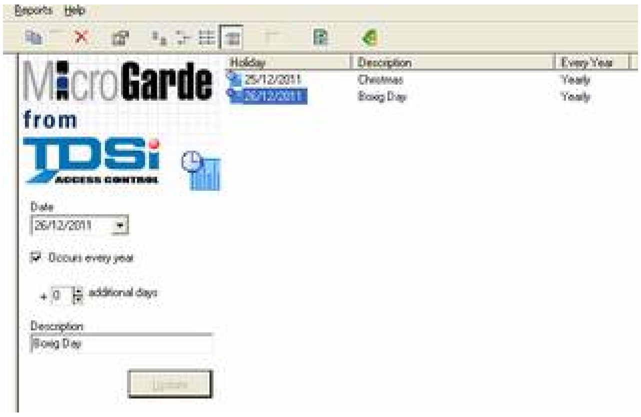
- *Full Rights*: If an operator has Full Rights to Operators then he or she will be able to change all of their other rights when they are logged on. Therefore only the most trustworthy person should have Full Rights to Operators.
- *User Rights*: Allows a general user operator setting which allows limited controlwith editing allowed for cards and cardholders.
- *View Rights*: these rights allow only to see the icons and objects and NO editing/deleting/adding enabled.
- *No Rights*: Choosing "No Rights" for any particular object mean that the Operator won't even see that they exist. If you click on an object, you can change the setting for that object in the Access Rights field.

5.11 Holidays

Holidays are used to control the behavior of time patterns on days when your company may be closed. MICROgarde allows you to specify any number of holidays from now and for the next few years. However the controller has a limited amount of memory and therefore only stores up to 50 at any one time. For the controller to be automatically updated, if you specify more than 50, this software package has to be running.

5.11.1 Viewing Holidays

To view existing holidays, choose **View > Holidays**. MICROgarde Explorer lists the defined holidays in the main display area.



Holiday	Description	Every Year
25/12/2011	Christmas	Yearly
26/12/2011	Boxing Day	Yearly

Date
26/12/2011

☑ Occurs every year

+ 0 additional days

Description
Boxing Day

Figure 80 Listing Holidays

5.11.2 Adding a New Holiday

1. Select the **New** button or right click in the main screen and select **New** from the context menu. A holiday is automatically inserted on the next available line.
2. Select the new holiday in the list.
3. Change the date as required.
4. Select **Occurs every year** if the holiday recurs on the same date each year. This will save adding the holiday again each year.
5. If the holiday extends for two or more days, use the **Additional days** control to dial the additional number of days in the holiday.
6. Click on **Update**.

5.12 Events

Events are messages generated - either by controllers or by software - to provide information; for example, when a card is used at a reader, or when an operator adds a new card holder into the database.

Events generated by a controller remain in the memory of the controller until they are "polled" by the MICROgarde communications service. Normally, if the MICROgarde computer is turned on (and someone is logged in if this doesn't happen automatically) then the communications service will be running in the background (look for the icon in the system tray) and events are polled almost immediately they have occurred.

If the computer is not continuously polling for events, the message will stay in the controller's memory until it is over-written by newer events. As the controller can hold 5000 events, the length of time an event message will remain in memory will vary. The software will store 45 days of events, after this time they will be deleted.

There is a full list of events on page 99.

5.12.1 Managing events

An event will be available for viewing or reporting only if:

- It is not disabled.
- The controller which recorded the event was polled before the event was overwritten by a newer event.
- It is less than 45 days old.

An access control system can generate many hundreds of events a day, and most of these will be perfectly normal occurrences. You may decide that you never need to see a message unless it relates to something that represents a security risk - for example, someone trying to open a door when they should know that they are not allowed to. Or, you may decide that you want to see all messages, but want to have your attention drawn to anything out of the ordinary. For these reasons, for each and every event you can define whether it will be recorded (i.e. recorded by the controller, and collected by the software) and if so, whether it is to displayed:

- *Disabled*: The controller never generates an event message for this event.
- *Normal*: The controller generates a message for the chosen event; the message appears in the event list when it is "polled" from the controller.
- *Abnormal*: As for "*Normal*", except the event will have an icon next to it in the event list, to draw attention to it. This acts as a kind of alarm icon to visually stand out in the event list.

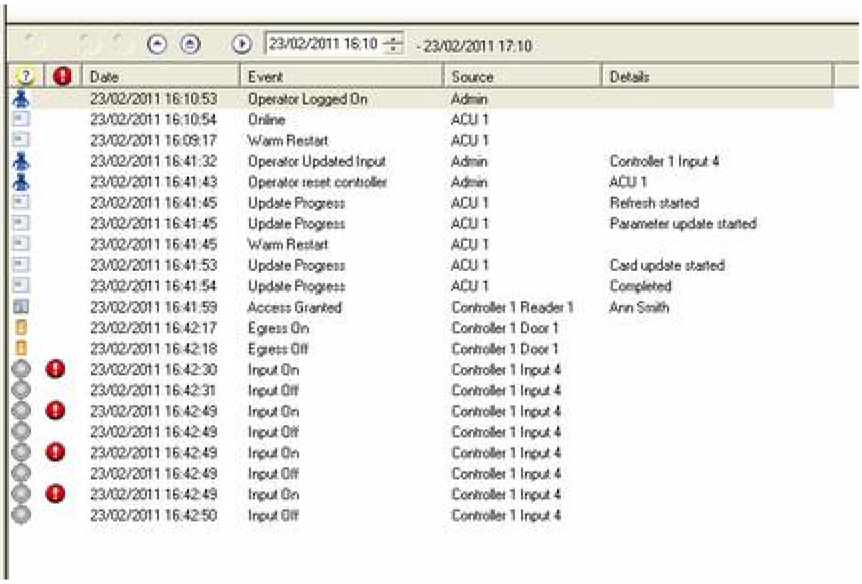
Note. Certain events can also cause a relay to operate: this is true whether or not the message is disabled. The events which can do this are highlighted in the list at the end of this page.

If you record every event then more disk space will be required than if you disable some events. This should not normally be a problem as the software automatically deletes events older than 45 days but bear in mind that backups will also require more disk space.

Provided an event is recorded in the database, you can create a report (for viewing, printing or saving) by clicking on Reports in the MICROgarde Explorer menu bar (see the next chapter).

5.12.2 Viewing historical events

The lower section of the MICROgarde Explorer screen displays events - either in "real time" or by selecting a specific time period to show past events. When you start MICROgarde Explorer, the event list will be in "real time":



23/02/2011 16:10 - 23/02/2011 17:10

?	❗	Date	Event	Source	Details
		23/02/2011 16:10:53	Operator Logged On	Admin	
		23/02/2011 16:10:54	Online	ACU 1	
		23/02/2011 16:09:17	Warm Restart	ACU 1	
		23/02/2011 16:41:32	Operator Updated Input	Admin	Controller 1 Input 4
		23/02/2011 16:41:43	Operator reset controller	Admin	ACU 1
		23/02/2011 16:41:45	Update Progress	ACU 1	Refresh started
		23/02/2011 16:41:45	Update Progress	ACU 1	Parameter update started
		23/02/2011 16:41:45	Warm Restart	ACU 1	
		23/02/2011 16:41:53	Update Progress	ACU 1	Card update started
		23/02/2011 16:41:54	Update Progress	ACU 1	Completed
		23/02/2011 16:41:59	Access Granted	Controller 1 Reader 1	Ann Smith
		23/02/2011 16:42:17	Egress On	Controller 1 Door 1	
		23/02/2011 16:42:18	Egress Off	Controller 1 Door 1	
	❗	23/02/2011 16:42:30	Input On	Controller 1 Input 4	
		23/02/2011 16:42:31	Input Off	Controller 1 Input 4	
	❗	23/02/2011 16:42:49	Input On	Controller 1 Input 4	
		23/02/2011 16:42:49	Input Off	Controller 1 Input 4	
	❗	23/02/2011 16:42:49	Input On	Controller 1 Input 4	
		23/02/2011 16:42:49	Input Off	Controller 1 Input 4	
	❗	23/02/2011 16:42:49	Input On	Controller 1 Input 4	
		23/02/2011 16:42:50	Input Off	Controller 1 Input 4	

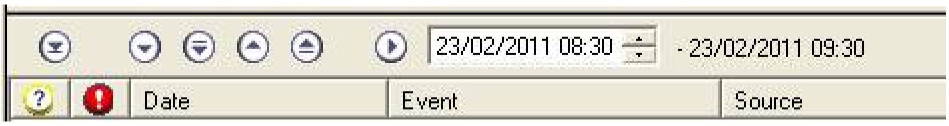
Figure 81 Events

The two left-hand columns display icons that represent the type of event (the icons match those in the short-cut bar), and Abnormal Event is shown as an ALARM icon.

Note that if polling has been off for some time, when it restarts the order in which the events will be displayed is not necessarily chronological. This is because MICROgarde will poll a few events from each controller in turn. However, once all events have been polled then navigating the list will always result in the events being shown chronologically.

The top of the event list features the following navigation buttons (left to right):

1. Display current events (i.e. real time, only events that were polled after you selected this option)
2. Skip forward 1 hour
3. Skip forward 24 hours
4. Skip back 1 hour
5. Skip back 24 hours
6. Jump to the specified time, and display the next 1 hour's events: you can “left click” on the Day, Month Year or Hour or Minute individually and click on the Up and Down arrows to scroll through. Alternatively you can just “left click on the date etc and type in the date required.



23/02/2011 08:30 - 23/02/2011 09:30

?	❗	Date	Event	Source

Figure 82 Event navigation controls

6. Reports

There are five types of reports:

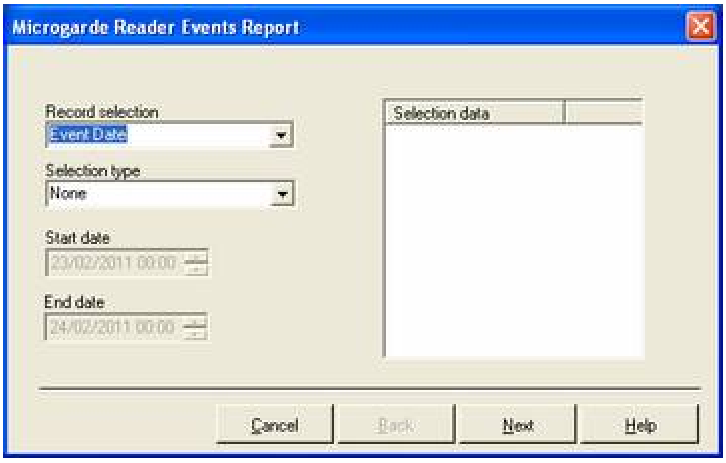
- **Location report**: A list of Card Holders and whether they are on-site or off-site (this is determined by a setting in each Reader's properties.
- **Event reports**: Events generated either by controllers (and by implication anything connected to a controller, such as a reader) or by Operators.
- **Card Holder reports**: A list of card holders in one of three formats: with information fields, with access rights, or with issued cards
- **Database reports**: A list of items in the database (other than Card Holders) selected by type.
- **Custom reports**: MICROgarde software allows new report templates to be installed without any need to update the software.

6.1.1 Creating a Report

To create a report:

1. Choose the appropriate type from the **Reports** menu.

   A Report dialog box is displayed: the layout of this will depend on the type of report you have chosen: As an example, a Reader Events Report is shown below.



Microgarde Reader Events Report

Record selection: Event Date

Selection type: None

Start date: 23/02/2011 00:00

End date: 24/02/2011 00:00

Figure 83 Creating a report

2. Choose the type of records to be included in the report from the *Record selection* dropdown list.

   - *Is equal to*: select one from the selection list (only this item will be selected)
   - *Is not equal to*: select one from the selection list (one item only)
   - *Is greater than or equal to*: select one from the selection list
   - *Is less than or equal to*: select one from the selection list
   - *Is between*: select two items from the selection list to determine the boundaries. This Note that between is the selection of the two items and will include both items selected AND all items in between that are in ALPHABETICAL order.

- *Is not between*: select two items from the selection list to determine the boundaries
- *Is one of*: select one or more items from the list, up-to a maximum of 10 items. Is not one of; select one or more items from the list, up-to a maximum of 10 items.

> **Note.** Windows multiple selection rules apply. To select several types, hold down the ctrl key and click on each item in turn. To select a group, left click on the first item in the list and then hold down the shift key and click on the last item.

3. The *Selection data* box is populated with a list of items based on the record selection. Depending on your chosen selection types, select one or more items from the list to complete the selection criteria.

   To see which items will be selected with some of the above criteria, you may prefer to click on the title Selection Data for that right hand side screen, to then place all the items into an ALPHABETICAL order first, before selecting.
4. Enter a *Start date* & *End date* for the reporting period.
5. Click on the **Next** button.
6. Depending upon your selection, you may be prompted to choose more selection criteria and you will be presented with a similar dialog box to that shown in Figure 83. If you do not want to apply any more selection filters, click on the **Next** button.
7. Most reports allow you to specify a sorting order for the report data. However, some reports are predefined because of how the data is calculated. If prompted, choose how you want the data to be presented in your report. The Events Report shown below allows you to choose primary and secondary sorting criteria to sort report data according to *Event Date*, *Event Description* or *Reader Name*.

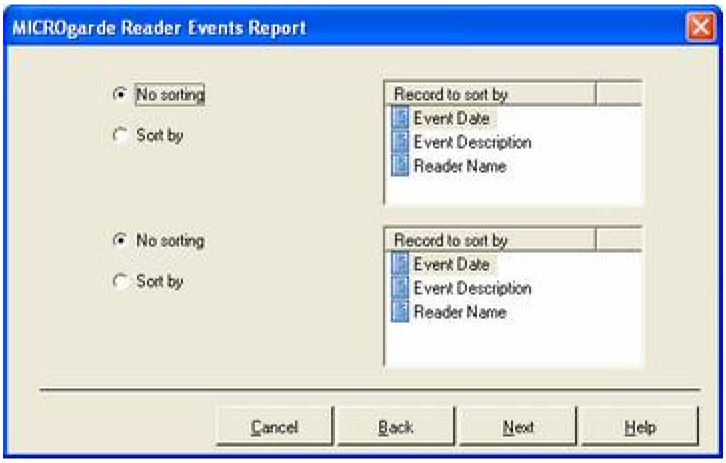
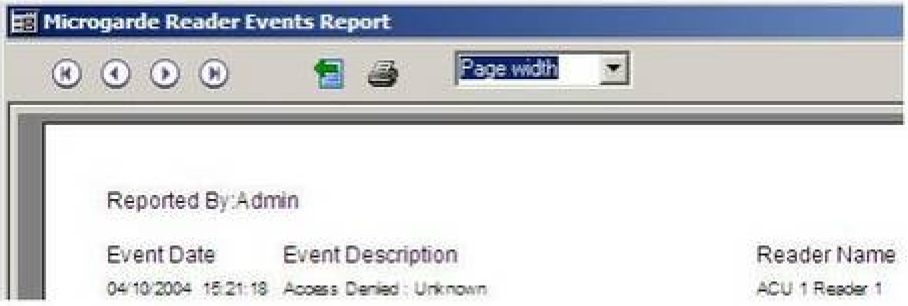


Figure 84 Sorting a report

8. Click on the **Next** button to continue.
9. Choose the destination for the report:
10. *Preview:* the report is shown on-screen. The preview window allows you to browse through the report and to export or print it.

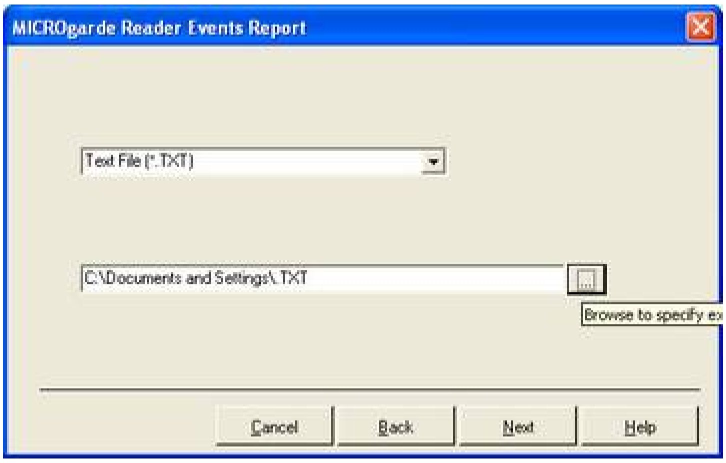


Reported By:Admin

Event Date | Event Description | Reader Name
04/10/2004 15:21:18 | Access Denied : Unknown | ACU 1 Reader 1

Figure 85 Previewing a report

11. *Export*: Choose from the list of available formats: CSV, HTML, DOC, PDF, RTF and TXT (PDF format may require the installation of a suitable third-party printer driver). Browse to the folder where you want to store the report and name the exported file.

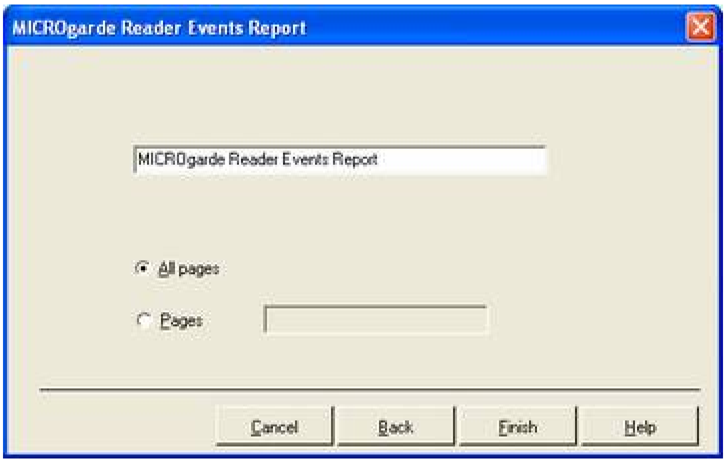


Text File (*.TXT)

C:\Documents and Settings\.TXT

Figure 86 Exporting a report

12. *Print*: Enter a name for the report (this is printed on each page) and choose whether to print all pages or a range of pages.



MICROgarde Reader Events Report

● All pages

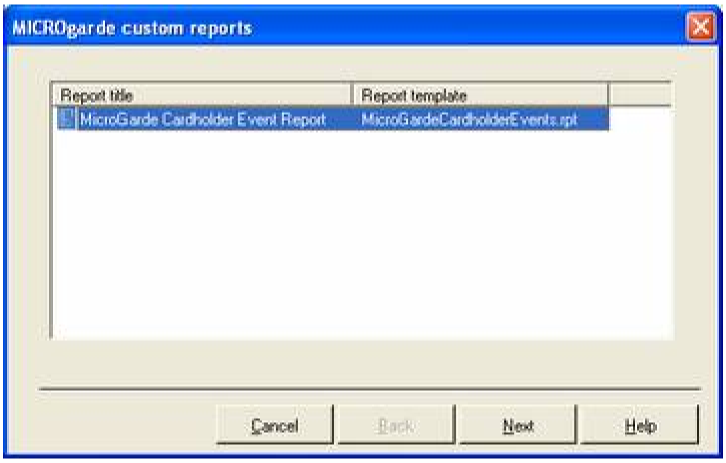
○ Pages

Figure 87 Printing a report

6.1.2 Custom Reports

New report templates can be supplied without any need to update the software. Contact TDSi for details.

If you order a custom report, two files (with .MCR and .RPT extensions) will be sent to you by TDSi. Copy these files into the *C:ProgramFiles/TDSi/MicroGarde/Reports* folder.You will then see the new report in the MICROgarde *Custom reports* list.



MICROgarde custom reports

Report title	Report template
MicroGarde Cardholder Event Report	MicroGardeCardholderEvents.rpt

Figure 88 Selecting a custom report

To use the custom report, select it and then click on the **Next** button.

Custom reports follow the same format as described in the previous section for standard reports.

7. Troubleshooting

This section describes some of the common problems that you may encounter and explains their solutions.

I've lost my password

In order to best preserve your security, we have designed the system so that there is no "back door" into the database for anyone except TDSi. You have two options:

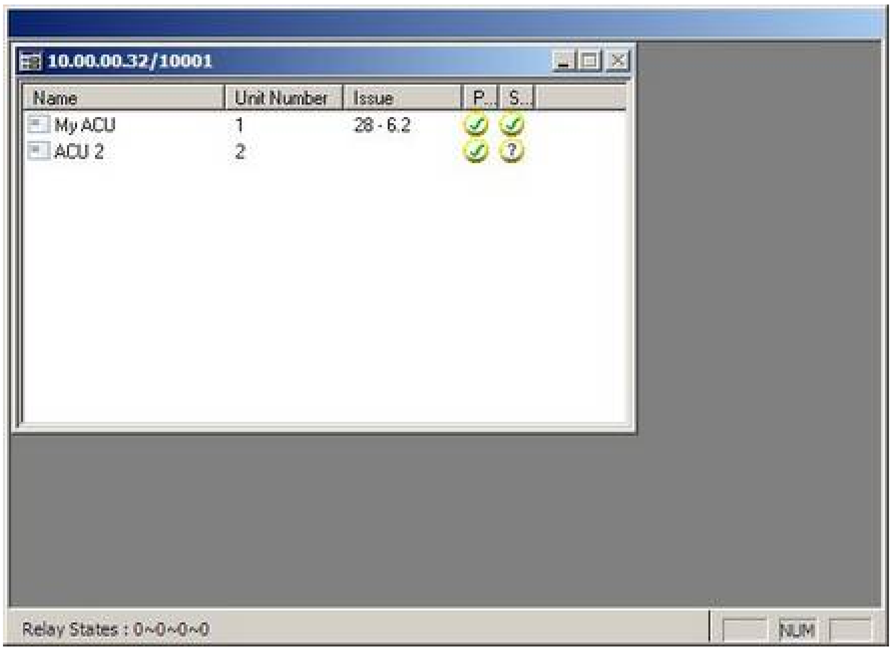
1. Un-install and reinstall the software, and re-enter all your data
2. Contact TDSi for advice. We may be able to help (this is a chargeable service).

New Controllers not being updated

If this is a new installation and your controllers are not being detected, try this fault-finding procedure:

1. Make sure that the first page in **System Settings** is set correctly for your installation; i.e. either the correct communications port or the correct MAC address and IP address for the controller.
2. Make sure that the connections are correct as shown in on page 12.
3. Make sure that MICROgarde Communications is running (see page 36).
4. Right-click the MICROgarde Communications icon in the Windows System Tray and select **Show Communications service**.

   The screen should look like this:



10.00.00.32/10001

Name	Unit Number	Issue	P...	S...
My ACU	1	28 - 6.2	✓	✓
ACU 2	2		✓	?

Relay States : 0~0~0~0

Figure 89 Communications Service

5. This means the communications is running (in this case, via serial port COM1). Any ACUs in the list are in the MICROgarde database; the Polling column tells you whether polling is turned on; the Status column tells you if the unit is responding. If you do not get the "*New ACU*" icon flashing but you

know that a controller is definitely connected correctly, carry on to the next step.

6. If the screen is blank and has the status message "*Connection to communications server FAILED*" then the MICROgarde polling service is not running.
7. Go to **Control Panel** > **Administrative Tools** > **Services**
8. Look for **MPOLL Service Vx.x**. The word "Started" should appear in the Status column. If not, right click on the name of the service and select **Start** to start it.
9. This step assumes you have checked your connections, and you get the first of the two screens above.
10. If more than one controller is connected to the communications line, disconnect all except the one closest to the computer. Reset the controller (see page 26). After the reset, look at the communications LEDs: red and green should both be flashing, indicating that the unit receiving and responding.

No communication with any controller (but used to work)

If you have more than one controller, and believe you are not communicating with any of them, try this fault-finding procedure:

1. Re-boot the computer, start MICROgarde Explorer and log-in.
2. Go to step 4 in the *New controllers not being detected* section above.

Communications with only some of the controllers

If you have more than one controller, and only see events from some of them, check the following:

Click on the **Controllers** icon in the shortcut bar and check the "On line" column in the Main Display area.

If all the controllers are shown as on-line, but you don't get any events from one, try refreshing it (right-click on the controller's name and select **Refresh**). If that doesn't solve it, check that event messages are not disabled (for example, if you don't see any "door open" events, open the properties for that door and look at the events screen.

If one or more of the controllers is shown as not being on line, go to the controller and check that:

- Power is on
- The rotary switch is set to the correct unit number as set in MICROgarde Explorer
- The connections are secure.

If all this is correct, then reset the controller (see page 26).

I think a controller has failed

If you suspect that a controller has failed in some way, and needs replacing, carry out the following checks. Many apparent failures are caused by disturbed connections or incorrect setting up. Occasionally, electrical disturbance can cause a controller to stop responding normally - this is very rare but easily resolved by a Reset (see below).

1. Is the power supply OK (check for the 5V led on the controller)?. If not, check the power supply is providing 10-14 Volts. If the voltage is low, use a

multimeter to confirm that the controller is not drawing more than 500mA - if it is then an abnormal load may be present. Disconnect each device from the controller one at a time to see what is causing the load.

2. If the power supply is OK, as a first step reset the controller (see page 26). Perform trouble shooting on communications if necessary. If you simply cannot get communications to work on this unit (but you can on others) try swapping controllers with one that is working - if the problem now occurs on the other controller then a wiring fault is the most likely cause. If the problem remains with the original controller then it may be faulty.
3. If communications is working, test inputs (by connecting each one in turn to 0V) to confirm that each one results in an event in the MICROgarde Explorer.
4. Use the exit button (if fitted) or a piece of wire to connect the exit button input to 0V to see if the lock relay operates. Repeat this for each door if the controller is controlling 2 doors. If the relay does not operate then this may indicate either total failure of the controller, or fused relay contacts - either way, the unit needs replacing.
5. If the previous test results were OK, the last thing to check is for reader problems. After the unit was reset, the reader LED should have been flashing at half second intervals. When you present a card, the flashing should change to 2 second intervals - if it doesn't then this could be a reader problem, connection problem, cable problem or controller problem. The best test after checking connections is to substitute each of the other three components (reader, cable, controller) in turn with known working components to see which is to blame.

A card isn’t being read

Reset the controller (see page 26) and follow the guidance in step 5 of **Failed controller** above.

A card doesn’t unlock door

If no card will unlock a door, it may be that the lock relay is not controlled off (the event list will say "access denied - door locked). Otherwise it may be a fault in the lock, or lock power supply, or lock connections. A further possibility is that the card was added into the system when communications was not running - start by performing a Refresh of the controller(s) in question.

If the problem is only with some cards, check the following:

1. Does using the card result in an event? If so, read the wording in the Event column in the Event list - this may give you clues that save you following the rest of this checklist.
2. Is the card issued to a card holder? (if so, their name will appear in the event list when the card is used).
3. Does that card holder have rights to use the reader at this time of day? Look at the card holder to see what their access level is; then look at the access level to see which readers are permitted, and following which time pattern; then look at the time pattern.
4. Is the card set to Lost, Damaged or Suspended, or has it expired? (click on the Cards shortcut and find the card in the Main Display in Details view)

No events in event list or reports

There are several possible reasons:

- There is a communication problem (see *No communications with any controller*).
- No events are being reported. For each object that should be generating events - reader, door etc., look at its properties by double-clicking on it in the Main Display and check that the events have not been disabled.
- In MICROgarde Explorer, the Event list is showing a time period for which there are no events.
- In Reports, no events match the selection (by date or otherwise)

The event list is not in chronological order

If polling has been off for some time, when it restarts the order in which the events will be displayed is not necessarily chronological. This is because MICROgarde will poll a few events from each controller in turn. However, once all events have been polled then navigating the list will always result in the events being shown chronologically.

People are allowed and denied access at the wrong times

The most likely cause is an Access Level Time Pattern that has been incorrectly entered. Note that a Time Pattern is a sequence of times, days of week and actions. If you have one line set to disable access at 1900 every day of the week, and another line to turn it on at 0700 Monday-to-Friday, then it will be disabled at 1900 on Friday and will not be enabled until Monday at 0700. This can be useful if intentional, but can cause problems if unintentional!

People are allowed through the wrong doors

First, refresh the appropriate controller(s) and see if the problem remains. If so, check the properties of the Access Level for the card holders affected.

Doors with Time Patterns are locked and unlocked at the wrong times

The most likely cause is an Relay Time Pattern that has been incorrectly entered. Note that a Time Pattern is a sequence of times, days of week and actions. If you have one line set to lock the door at 1900 every day of the week, and another line to unlock it at 0700 Monday-to-Friday, then it will be lock at 1900 on Friday and will not unlock until Monday at 0700. This can be useful if intentional, but can cause problems if unintentional!

7.2 Restoring a Backup

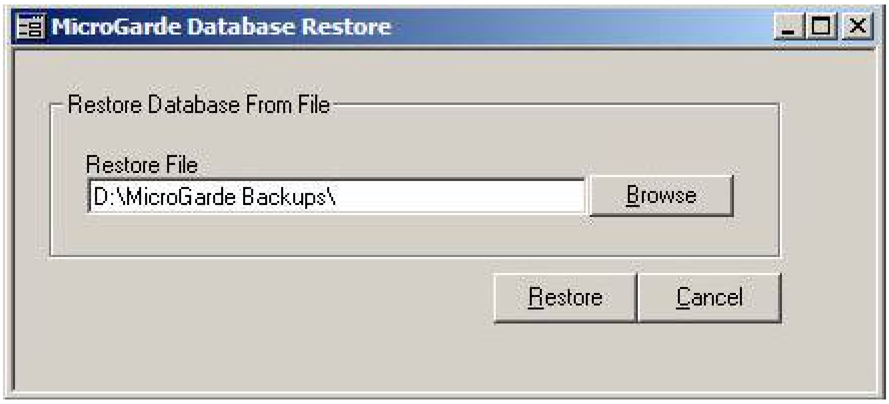
Note. When you restore a backup, it will overwrite your existing data. Any changes you have made since the backup was made will be lost unless you make another backup first. In particular it is important to realize that Operators and their passwords will also have been restored, and that any changes to these since the back-up will have been lost.

To restore a backup:

1. Close MICROgarde Explorer.
2. Shut down the MICROGarde Communications Server (right-click on its icon in the System Tray and choosing **Exit**).
3. Run MICROGarde Restore??? (from the Start menu:

   Start > All Programs > TDSi, > MICROgarde > MICROgarde Restore???

   The MICROgarde Database Restore dialog box is displayed.



D:\MicroGarde Backups\

Figure 90 Restoring a Backup

4. Browse to the backup file you want to use, and click **Restore**.

The process takes a few minutes; at the end you will see a message confirming that the database has been restored.

8. Technical Information

8.1 Specification

Table 16 MICROgarde specification

	MICROgarde 1	MICROgarde 2
Size (box)	Non-PSU version: 210 x 135 x 47 mm	
	PSU Version 346 x 280 x 85 mm	
Temperature range	-5°C to +50°C	
Power	Non-PSU version: 10-14V @ 1A	
	PSU Version: Input: 220 to 240 VAC, 80 VA. Output: 13.8 VDC, 2 A total. Back-up battery charging facility Input: 220 to 240 VAC, 80 VA.	
Cards	5000 with MICROgarde software 10,000 with EXgarde software	
Door control	0 or 1	0, 1 or 2
Communications	RS232 (with built-in RS485 converter for downstream units)	
	RS485	
	Optional TCP/IP module adds 10/100mbps Ethernet port	
Readers	0-2	0-4
Inputs	4 in total :	4 in total :
	4 spare in 0-door configuration	4 spare in 0-door configuration
	2 spare in 1-door configuration	2 spare in 1-door configuration
		0 spare in 2-door configuration
	Optional I/O module adds 4 inputs (and 2 relays)	
Outputs	2 (30V, 2A rating) in total	2 (30V, 2A rating) in total :
	2 spare in 0-door configuration	2 spare in 0-door configuration
	1 spare in 1-door configuration	1 spare in 1-door configuration
		0 spare in 2-door configuration
	Optional I/O module adds 2 relays (and 4 inputs)	
Features	0 or 1 door controller	0, 1 or 2 door controller

	MICROgarde 1	**MICROgarde 2**
(Controller)	2 readers (using Clock&Data or Wiegand 26-bit or Wiegand 37-bit interface)	4 readers (using specified TDSi readers) or 2 readers (using Clock&Data or Wiegand 26-bit or Wiegand 37-bit interface
Shared Features (Controller)	1,000 event capacity -- Anti-passback (timed or true) -- Man-trap -- Built-in tamper switch on controller board	
	Mains fail and low battery detection -- Reader removal detection -- 16 time groups for access rules	
	Card, Card+PIN and PIN-only security modes -- Scheduled operation of relays, including lock relays	
	Flash-uploadable firmware -- Multi-card access mode for accompanied access	
Shared Features (MICROgarde Software)	Up to 200 controllers -- Automatic detection and configuration of controllers and readers	
	45-day on line event database -- Automated back-up	
PC Specification	Workstation grade architecture 32-bit operating system 32-bit/64-bit processors – Intel Core i5 Sandybridge or above Virtual PC environment not supported 4GB RAM 100MB-BaseT network interface or above	

8.2 Glossary

Table 17 Glossary

Access Mode	Reader Access Mode.
Access Control Unit	An electronic board that is connected directly to readers, locks etc., and that contains a list of all the cards and rules that determine whether a card holder will be allowed through a door.
ACU	Access Control Unit (Controller).
Access Level	List of readers and time patterns, that determine the access rights of all card holders allocated to the Access Level.
Anti-passback	A high security mode of access, where a card may be prevented from being used at the same reader twice, thus preventing a card from being passed back (through a window or turnstile) for use by another person. A door with a reader on either side can utilize "true" anti-passback where the card must be used at alternate readers. A door with one reader can utilize timed anti-passback, where a second presentation of the card is inhibited for up to 24 hours.
Alarm	An event which is treated differently from a non-alarm event, so as to draw to your attention.
Archive	The act of exporting an event report to a file, so that those events may be viewed after the 45-day limit that applies to Reporting and the Event List.
Backup	The act of making a copy of the entire database (including events) to safeguard against loss or damage to the working database.
Controller	MICROgarde unit or Access Control Unit (ACU).
Card-holder	A person defined within the Card Holders section of the MICROgarde software. The person may not actually have a card issued to them, or they may use only a PIN to gain access.
Card	In the context of the access control system, any number that indicates the identity of a person. This may be a PIN with no physical object associated with it.
Card+PIN	A higher-security access mode (compared with card-only), where after presenting a card, a PIN (personal identification number) must be typed in at the keypad next to the reader. Each card has its own PIN, stored in the memory of the controller.
Digital input	An input that is connected to a device that can only signal "open" and "closed"
Event	Message that is displayed as a result of a system process e.g. a card is used, a door opens, an operator adds a card.
Forgiveness	An automated re-set of the *anti-passback* status of every card at a set time of day.
Input	A connection to a controller that can be used to report a change in another piece of equipment (usually a switch of some sort). An input may be configured to monitor a "supervised" or "digital" circuit.
LED	Indicator light (abbreviation for Light Emitting Diode) fitted to readers and controllers.

Mantrap	A high security mode of access, which can be enforced by a single controller that controls two doors, and where the doors are fitted with sensors. Access through one door (by card or exit button) will not be allowed unless the other door is shut.
Message	The text that describes an event and therefore that appears in the Event List and/or an Event Report. The term "Message" and "Event" are often regarded as the same thing.
MG	Short term for MICROgarde
MG1	Alternative term for a MICROgarde I controller
MG2	Alternative term for a MICROgarde II controller
On-line	A controller is on-line if it has been detected by the MICROgarde background communications software. Polling must also be enabled for polling to occur.
On-site	If a card holder is shown as "on site" then the last reader they used was set in the database to be an "on site" reader.
Off-site	If a card holder is shown as "off site" then EITHER the last reader they used was not set in the database to be an "on site" reader or an operator has set the card holder as off-site. New card holders are always shown as off site until they use an on site reader.
PIN-Only	A lower security access mode (compared with card-only), where it is necessary only to type in a PIN (personal identification number) at the keypad next to the reader. More than one PIN may be valid at any time, but a PIN must be associated with a Card Holder in order to be valid (i.e. stored in the controller's memory). As more than one person might know a given PIN, you cannot rely on the name that appears in the event list as being the admitted person.
Polling	The background communications between the computer and a controller, that collects events from the controller
Pop-up menu	The menu of options that appears when you right-click an object (e.g. reader, door, card holder) in the Main Display.
Reset	The process of causing a controller to return to its factory settings
Reader Access Mode	A setting that determines what is needed for the door to unlock. Reader Access modes are:Card+PIN, PIN-only, Supervised Entry and Anti-passback. When Card+PIN is off, then entry is by card only. Mantrap is not a Reader Access Mode - it is a Door property.
Relay	A component of the controller that can be used to control another piece of equipment
Refresh	The act of sending all relevant data to a controller, to ensure it has all the information and cards (and only such information and cards) that are currently defined in the database.
Supervised entry	A high security mode of access, where two or more card presentations may be required before the door is unlocked.
Supervised input	An input connected to a device that uses resistance to indicate tampering as well as the normal "open" and "closed" events
Time pattern	A schedule of times and days of the week that can cause changes to relays, reader access modes or access levels

8.3 Events

This section lists the event messages that may be reported by MICROgarde Explorer:

Access Denied : Anti-pass Back Enforced
Access Denied : Door Locked
Access Denied : Expired
Access Denied : Invalid PIN Entered
Access Denied : Invalid PIN Entered Too Many Times
Access Denied : Man Trap Enforced
Access Denied : No PIN Entered
Access Denied : Not Valid In Reader
Access Denied : Access Level Disabled
Access Denied : Unknown
Access Granted
Card and PIN Time Control Off
Card and PIN Time Control On
Card Only Time Control Off
Card Only Time Control On
Card update started
Completed
Control Feature Off
Control Feature On
Counter Above Limit
Counter below limit
Counter Timed Reset
Door Ajar Alarm
Door Ajar Pre-alarm
Door Closed
Door Forced Open
Door Opened
Multi-card access Time Control Off
Multi-card access Time Control On
Multi-card access Primed
Multi-card access Timed Out
Duress PIN Entered
Egress Off
Egress On
Extra Event Data
Firmware update started
Input Closed Circuit
Input Off
Input On
Input Open Circuit
Input Undefined Event
Local Login
Mains OFF
Mains ON
Offline
Online
Operator changed card status
Operator Created New Controller
Operator Created New Access Level
Operator created new card
Operator created new card holder
Operator created new operator
Operator Created New Port

Operator Created New Time Pattern
Operator Deleted Controller
Operator Deleted Access Level
Operator deleted card
Operator deleted card holder
Operator deleted operator
Operator Deleted Port
Operator Deleted Time Pattern
Operator executed report
Operator Logged Off
Operator Logged On
Operator refreshed Controller cards
Operator refreshed Controller parameters
Operator refreshed Controller
Operator Updated Controller
Operator updated Controller polling
Operator Updated Access Level
Operator updated card
Operator updated card holder
Operator Updated Counter
Operator Updated Door
Operator updated door control
Operator Updated Input
Operator updated operator
Operator Updated Port
Operator Updated Reader
Operator updated reader access mode
Operator Updated Relay
Operator updated relay control
Operator updated system settings
Operator Updated Time Pattern
Parameter update started
PIN Only Time Control Off
PIN Only Time Control On
Reader Error
Refresh started
Relay Time Control Latched Off
Relay Time Control Latched On
Relay Time Control Off
Relay Time Control Pulsed
Slave Off Line
Slave On Line
Summer Time Ends
Summer Time Starts
System Failure
Tamper Switch Error
Tamper Switch Ok
Time Group Disabled
Time Group Enabled
Unknown Counter Event
Unknown Door Event
Unknown Input Event
Unknown Operator Event
Unknown progress
Unknown Reader Event
Unknown Relay Event
Update Failure
Update Progress
Warm Restart (occurs if power is turned off at a controller, then back on again)

8.4 Compliance Notices

8.4.1 Compliance with CE regulations

The equipment is designed, tested & declared to conform to the following CE directives:-

89/336/EEC	EMC Directive
93/68/EC	Low Voltage Directive

The equipment has been tested & found to comply to the following EMC & Safety standards:-

Electromagnetic emission	EN 55022:1998, Class B
Electromagnetic emission	FCC CFR47, Pt15.107 & .109, Class B
Electromagnetic immunity	EN 50130-4:1995, Class A
Safety of IT Equipment	EN 60950: 1998

Limitations on the intended operating environment

The equipment is intended for use in access control applications in a wide range of configurations. It is intended for use with third party equipment attached at the power supply input, the reader inputs, various control outputs and the data communications ports. Such third party equipment, and all cabling must be of suitable design and installation to ensure that the overall system complies with the requirements of the EC EMC directive.

Guidance notes for the installation and use of TDSi equipment must be strictly followed. Due to the wide range of access control products TDSi notes cannot cover all possible type and combinations of equipment that may be assembled to form a total system.

TDSi exercise due diligence to ensure that its equipment is suitable for use in the stated applications, but ultimate responsibility for the compliance of a complete system must rest with the prime contractor at a site where local conditions may require additional EMC precautions to be taken.

Connection of external power supplies

To comply with CE Access Control specification requirements we advise that the equipment is operated from BATTERY BACK UP mains power supplies to ensure operation is maintained over short mains supply interruptions.

Any external power supply being used to drive the equipment, or being switched by the equipment must be independently protected against overload to prevent possible damage during fault conditions that may exceed the equipment maximum ratings.

To limit interference the mains supply inputs of any external, AC mains power supply must be fitted with 470pf, Class Y, mains suppression capacitors as supplied in the installation kit. The capacitors should be connected from line to earth and from neutral to earth as shown.

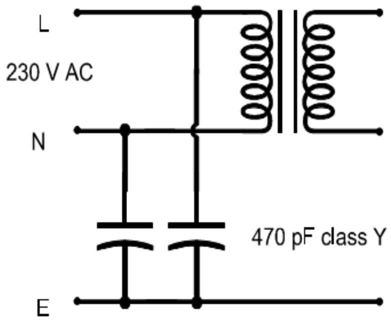


Figure 91 Use of suppression capacitors

8.4.2 FCC Regulations Notice

This device complies with Pt 15.107 & .109 of the FCC CFR47regulations.. Operation is subject to the following two conditions:-

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

WARNING! CHANGES OR MODIFICATIONS TO THIS UNIT NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THIS EQUIPMENT.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Pt 15.107 & .109 of the FCC CFR47 Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instructions, may cause interference harmful to radio communications.

There is no guarantee, however, that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

8.4.3 CSA EMC Notice

This digital apparatus does not exceed the Class B Limits for radio frequency emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n’émet pas de bruits radioélectriques dépassent les limites applicable aux appareils numériques de la Class B prescrites dans les règlement sur le brouillage radioélectrique édicte par le Ministère des Communications du Canada.

8.4.4 Safety Notices

Product description

These notes apply to TDSi MICROgarde Access Control Units when driven from an external, third party, mains power supply. The mains supply must be connected to the equipment by a permanently connected wiring installation as described below.

Rating

The TDSi MICROgarde Access Control Units, without built-in Mains PSU, draw a maximum of 150mA from the low voltage (10 to 14V) DC supply, but may be connected to readers, lock-strikes or ancillary equipment that draw substantially more current. The system designer or installer must ensure that the power supply, or power supplies used to drive the system are of sufficient capacity to drive the whole system, and that they are installed correctly.

Safety WARNING:

⚠ **CAUTION! DISCONNECT THE MAINS SUPPLY BEFORE REMOVING THE COVERS OR MAKING CONNECTIONS TO THE EQUIPMENT.**

All regulations and requirements MUST be must strictly followed to prevent hazards to life and property both during and after installation, and during any subsequent servicing and maintenance.

Positioning and fixing of equipment

The equipment must not be installed out of doors or in damp or exposed conditions.

To ensure mechanical stability the equipment must be secured using appropriate fasteners or brackets to a wall, pillar or other part of the building structure, or to associated, stable equipment.

The equipment must not be sited near to sources of heat. It is designed for use in ambient temperatures ranging from 0 to 40°C.

Connecting a permanently wired mains supply to the equipment.

Ensure that the mains supply to associated equipment or power supply is SWITCHED OFF before starting any wiring. Wiring should be in accordance with the current I.E.E. regulations, or the appropriate standards in your country, and should be performed by a properly qualified electrician. For permanently connected equipment a readily accessible disconnect device shall be incorporated in the fixed wiring.

Any mains wiring should be via a switched, fused spur with a 3A fuse (UK) rating, and should use approved 3 core mains cable of minimum cross section area 0.75 sq mm. The installation MUST be provided with a double pole isolator switch with a contact separation of at least 3mm.

Connecting signal wiring to associated equipment.

TDSi MICROgarde Access Control Units must be connected to other equipment forming part of an overall control system using signal wiring connections made with screened cable with the screen securely connected to an earth point at the controlled equipment end and at earth points within the MICROgarde equipment. Where individual remote equipment is locally earthed it is permissible to disconnect the cable screen earth connection at one end of the cable. Certain simple control signals to inputs and relay control lines may be connected using unscreened cable, but remote equipment must be independently and correctly connected to a safety earth

Internal fuse rating

The MICROgarde main logic PCB is fitted with fuse protection marked FU1. In case of failure FU1 should be replaced with a 1A Anti-surge, 20mm Fuse (TDSi part number 2021-0030).

Lithium cell

A Lithium cell is fitted in a battery holder on the MICROgarde main logic PCB and will support the memory and Clock functions for a maximum of 10 years in normal environmental conditions. The cell will not normally need to be changed during the normal life of the product, but may need to be replaced if the unit is left un-powered for very long periods. The Lithium cell used is a type CR2032 (TDSi part number 2020-0015)

If it is necessary to change the cell ensure that it is fitted correctly as shown in the diagram below:

⚠ **CAUTION! DANGER OF EXPLOSION IF CELL IS INCORRECTLY REPLACED!**

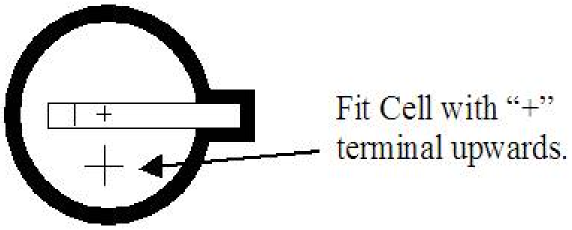


Figure 92 Fitting a lithium cell

ℹ **NOTE.** Dispose of used cell according to the manufacturer's instructions

TDSi ACCESS CONTROL

EC DECLARATION OF CONFORMITY

EQUIPMENT: MICROgarde Series Access Control Units

MODEL No: 5002-18xx & 5002-19xx

MANUFACTURER: Time and Data Systems International Ltd

ADDRESS: Nuffield Rd, Poole,
Dorset, BH17 0RE
England

This is to certify that the aforementioned equipment fully conforms to the protection requirements of the following EC Council Directives on the approximation of the laws of the member states relating to:

Applicable Directives:	Title:
89/336/EEC	Electromagnetic Compatibility
93/68/EC	Low voltage

by the application of the following Technical Construction File (TCF) No: MICROgarde ACU TCF Issue 1

and in consideration of the following Standards: EN-55022:1998: Electromagnetic emission
EN-50130-4:1995: Electromagnetic immunity
EN-60950-1:2001: IT Equipment Safety

COMPETENT BODY:

EMC PROJECTS LIMITED
HOLLY GROVE FARM
VERWOOD ROAD, ASHLEY
RINGWOOD
HAMPSHIRE
BH24 2DB
ENGLAND

REPORT/CERTIFICATE No: 5807/04 & 05/264

Signed: M. Sussman
(Responsible person)

Position: Technical Director

Name: M P Sussman MBA, CEng, MIEE

Date of Issue: 13/1/2005

Time and Data Systems International Ltd
Unit 10 Concept Park
Innovation Close
Poole
Dorset
BH12 4QT
UK

t: +44 (0)1202 723535
f: +44 (0)1202 724975
w: http://www.tdsi.co.uk/

Sales Enquiries:	sales@tdsi.co.uk
General Enquiries:	info@tdsi.co.uk
Marketing Support:	marketing@tdsi.co.uk
Technical Support:	support@tdsi.co.uk